STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

Network Feasibility Study

March 1997

ECG
MANAGEMENT
CONSULTANTS

ECG MANAGEMENT CONSULTANTS
1111 Third Avenue, Suite 2700
Seattle, Washington 98101-3201
(206) 689-2200
FAX (206) 689-2209

EAST COAST OFFICE:
WAKEFIELD, MASSACHUSETTS

TABLE OF CONTENTS

TABLE OF CONTENTS

(continued)

TABLE OF CONTENTS

(continued)

I. EXECUTIVE SUMMARY

I. EXECUTIVE SUMMARY

A. BACKGROUND

Over the last several years, more and more emphasis has been placed on the need for accurate, timely, and complete criminal justice information. Both state and private entities are beginning to rely on the validity of criminal justice information to guide decisions on the acquisition of personnel, placement of personnel and facilities, and investments to be made in enterprise development. To obtain complete information, these entities must have access to information maintained by a variety of agencies involved in criminal justice. The criminal justice community has learned that to accomplish information sharing, all members of criminal justice agencies (federal, state, and local) must form partnerships and participate in creation and maintenance of the information used to guide, control, and monitor offenders in the state of Washington. The heart of this integration must focus around a Justice Information Network (JIN) that will allow the sharing and exchange of information between all jurisdictions.

At the same time, many criminal justice jurisdictions have made extensive investments in the use of technology in terms of computers, personnel, software, support facilities, and telecommunication networks. Consideration of future developments in technology must respect these current system investments, and future solutions must be cost-effective and beneficial to the community served. Therefore, the question was whether a network could be established to facilitate the exchange of information between criminal justice agencies without destroying the integrity of the systems currently in place. To evaluate the feasibility of establishing a common justice information network that would meet the needs of the criminal justice community, the Office of Financial Management (OFM) and the Executive Committee for Implementation of the Criminal Justice Information Act (Executive Committee) initiated a study to determine the feasibility of migrating toward a wide area network (WAN) or JIN that would support the above-noted needs.

B. PURPOSE OF THE STUDY

The JIN Feasibility Study was initiated to review the likelihood of establishing a common network environment that would support current, as well as future, criminal justice network needs. The study entailed identification and definition of the design, implementation costs, and administration framework required to make this network a reality. Specific objectives for this project included:

- Determining the interest and willingness of local criminal justice agencies to participate in a shared JIN.

- Identifying the technical readiness of local county infrastructures to connect to a shared JIN.
- Determining the costs and effort required by local jurisdictions to prepare for and connect to a shared JIN.
- Refining the design of the new JIN based upon Wide Area Network (WAN) technologies.
- Defining the security requirements and possible infrastructure required to operate the JIN within the context of the criminal justice environment.
- Assisting the state in defining the management and operational frameworks required to administer the WAN.
- Developing a plan for implementation of the JIN.

The project scope included all the major criminal justice agencies except for juvenile services and tribal courts.

C. CURRENT ENVIRONMENT

In today's environment, the Department of Information Services (DIS), Department of Corrections (DOC), and Department of Licensing (DOL), Office of the Administrator for the Courts (OAC), and the Washington State Patrol (WSP) provide networked linkage to over 70 percent of the criminal justice agencies served today at 852 different physical locations. The remainder of the criminal justice agencies have a variety of methods for gaining access to desired databases and information.

The current network infrastructure comprises separate data communication networks to connect to local and state organizations within the same geographic areas. These networks are primarily slow, proprietary, single-purpose networks. The annual recurring cost of maintaining this complex networked environment is approximately $232,000. Although the multiple networks operate today, they have the following deficiencies:

- Current networks have reached capacity and limited functionality. Additional capital must be invested to increase capacity.
- The need to exchange fingerprint, document, and photo images requires increased network capacity and new networking protocols. The implementation of advanced electronic mail services also requires increased capacity and functionality.

- Different protocols are used to support user needs, and movement to a standard protocol is difficult. Lack of adherence to new standards necessitates increased investment in network support.
- Multiple pieces of hardware and software are required to run the multiple networks. Movement to a JIN will reduce the need for duplicated resources.
- Access to state data repositories is difficult through the current multiple network environment. Personnel attached to one network cannot access data or information on another.
- Governance and administrative procedures for control and operation of multiple networks are inefficient and impossible to understand.

D. PROPOSED JIN

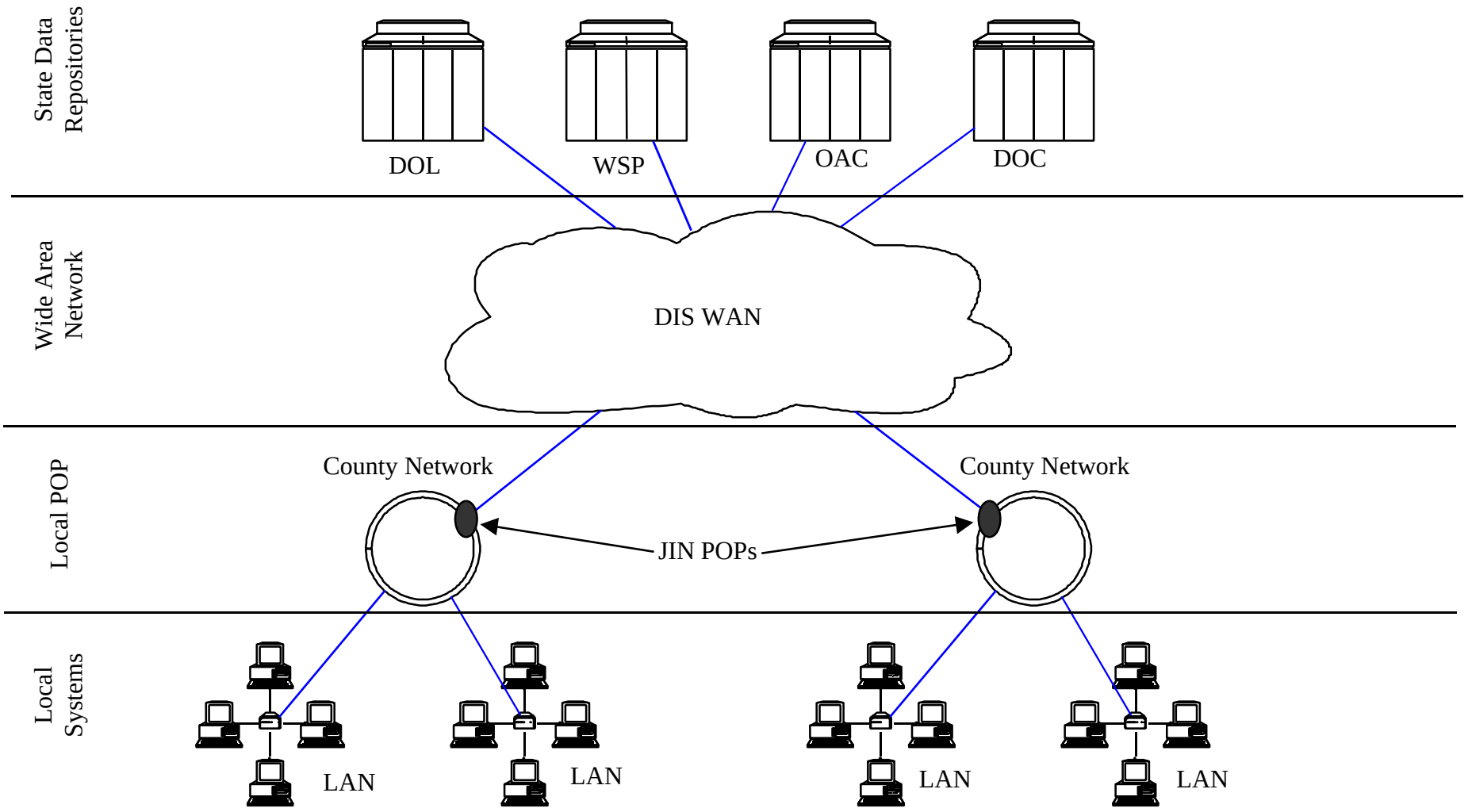
The proposed JIN is an advanced state and local networking infrastructure operating in conjunction with the state's current telecommunications network. This new logical network is composed of three separate components. As shown in EXHIBIT i, which follows this page, the proposed JIN design includes the following components:

- State Data Repositories: The databases included in the DOC, DOL, WSP, and OAC, and others.
- Wide Area Network: The communications transport available to transfer data and images to and from the state repositories to the users located in the counties.
- Local Jurisdiction Points of Presence (POP): The hardware and software available at the local level to migrate city and county networks into an integrated JIN.

Under the proposed JIN design, users will be able to gain access to the Wide Area Network (WAN) through local jurisdiction POP and then be able to access data resident in the state repositories. At the same time, standard message exchanges and transmission of images would occur between all criminal justice agencies authorized to participate in the JIN.

Critical to the operation of the JIN is its ability to meet agency requirements for performance and security. Implementation of a shared network infrastructure, even one of increased speed and bandwidth, can potentially restrict an agency's ability to operate at an acceptable performance level. In order to maintain agency information privacy, the implementation of JIN will require a significant investment in network security technologies.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
PROPOSED JIN DESIGN



ECG MANAGEMENT CONSULTANTS

E. ESTIMATED COSTS AND BENEFITS

The development cost of JIN is estimated at $4,160,698 over a 5-year implementation time frame. The capital equipment cost of JIN is $1,421,799; the network software cost is $771,080; the network security cost is $1,265,000; and the network operating cost is $3,167,950. This is an over fourfold increase in network operating costs from the current network cost of $992,748.

The estimated one-time cost for an agency to attach to JIN is estimated to be between $8,000 and $125,000 based on the level of technology used by the agency. The concurrent estimated recurring cost to maintain the implemented hardware is from $10,000 to $90,000. Lastly, software costs can range from $11,000 to $150,000 based on the desired level of utilization by the agency. In summary, the one-time cost for gaining access to the JIN would range from $20,000 to $275,000, and yearly operating costs would range from $10,000 to $90,000.

While the cost of the comprehensive JIN is very significant, it may be less expensive than each agency implementing its own new network, which has in effect already began. The estimated systemwide benefits of JIN are based on the utilization of automated information exchanges rather than manual methods of transferring information between agencies and can range from as little as $50,000 to several million dollars.

F. IMPLEMENTATION PLAN

The complete implementation of JIN would require up to 5 years to complete, since some state agencies would have to replace their existing hardware and software environments in the counties. The full utilization of a JIN would also require the parallel replacement of other key criminal justice application systems (ACCESS, WASIS, etc.) in order to achieve the desired benefits.

The JIN would be implemented based upon the readiness and networking capabilities of the county and local governments. In some cases, network costs can be reduced immediately through replacement of a multitude of current telecommunications lines with a shared multiprotocol network. The four phases included in the implementation plan are:

- Phase I - Project Planning - The first phase completes the project planning and establishes an overall governance structure, a project management organization, and a project manager. Issues related to network management, cost allocation, and operation would be outlined during this phase.

- Phase II - Detailed Network Design - The second phase updates the network implementation design based upon county readiness. Specific hardware and software requirements would be defined for each of the 39 county network infrastructures.

- Phase III - Product Evaluation - The third phase evaluates the potential products identified and selected for implementation of the network. This will allow the criminal justice agencies to verify the management and security features of the proposed network design.

- Phase IV - Network Deployment and Migration - The last phase of the project involves update of the detailed migration plan and purchase and installation of the new network infrastructure. This installation will take between 2 and 5 years depending upon the hardware and software readiness of the included agencies.

These steps or phases migrate the state toward an integrated city/county/state network infrastructure that will facilitate the exchange of multiple types of information. While the potential costs of operating such a network are significant, the criminal justice community cannot stand still as state agencies are currently implementing a new network regardless of whether a coordinated plan is in place.

II. BACKGROUND AND NEEDS ASSESSMENT

II. BACKGROUND AND NEEDS ASSESSMENT

Washington State seeks to improve the effectiveness of its criminal justice system - to promote public safety, to ensure the fairness of the justice system, and to make the most of limited criminal justice resources. As a part of this effort, OFM and the Executive Committee desire to improve and facilitate the electronic exchange of criminal justice information. This report identifies and documents the design, costs, and management framework required to propose implementation of a new multiprotocol WAN project to the state legislature.

A. BACKGROUND

Over the last 13 years, the Executive Committee has worked to improve the accuracy, completeness, and timeliness of criminal justice information within the state. As a result of the strategic and tactical plans for criminal justice records improvement developed in 1991, the Executive Committee created the policy-level Justice Information Committee (JIC) in 1992. This year JIC has identified eight key business goals or objectives to be accomplished over the next 4 years:

- Define the process control number (PCN) business rules and implement them in one or more counties.
- Have the Office of the Administrator for the Courts (OAC) receive felony and misdemeanant dispositions with PCNs from the counties, then supply these dispositions electronically.
- Define a solution for the capture of nonfiled dispositions.
- Replace the current Washington State Patrol (WSP) Identification Section criminal history computer system.
- Complete the first phase of the Electronic Arrest Reporting System.
- Replace the Washington State Crime Information Center (WACIC) computer system to include "value added" improvements and automated warrant transfer.
- Define a solution for the problem of multiple aliases for an individual within many of the state criminal justice information systems.
- Implement the Washington Association of Sheriffs and Police Chiefs Incident-Based Reporting System.

To enable the state to meet any or all of these objectives, the Executive Committee and JIC subsequently defined a telecommunications infrastructure project. The purpose of this project is to define and implement a modern multiprotocol network to support the collection and dissemination of criminal justice record information. This document represents the preliminary feasibility analysis supporting the implementation of such a network infrastructure.

B. PROBLEM/OPPORTUNITY STATEMENT

Individual criminal justice agencies currently support logically separate data communication networks to connect to local and state organizations within the same geographical areas. These networks are primarily slower, proprietary, single-purpose networks. While these networks allow each agency, such as the Department of Corrections (DOC), to support its own organization functions, they do not allow for communication at the local level between the agencies supporting the different criminal justice functions (for example, WSP personnel cannot communicate directly with the DOC community corrections office within the same county or city). Some counties and cities have started to implement metropolitan area networks (MANs) to improve data sharing and communications within a given geographical area, but still must maintain their multiple existing network lines to the various state agencies.

New data communications technologies provide the state with the opportunity to develop a high-speed consolidated JIN that would connect all the various organizations participating in the criminal justice life cycle. These new technologies include the application of fiber-optic cables for maximum network speed and capacity, the use of multiple protocols simultaneously along the same network lines, and the ability for a variety of information to be routed along the network. All types of data could be transferred across these new lines, such as document images, photographs, and fingerprints.

C. NEEDS ASSESSMENT

The primary goal for JIN within the criminal justice community is to access and exchange information among organizations across the state. This goal is articulated by the following two primary business objectives of the JIN project:

- Increase access to centralized criminal justice data.

  This requirement is twofold. The first need is to provide access to a number of criminal justice users who currently do not have direct access to centralized information (prosecuting attorneys, etc.). The second need is to provide users with access to more data sources or information.

- Increase data sharing between local and state entities.

  There is limited capability to exchange information directly between criminal justice organizations within a local jurisdiction or between local jurisdictions. Advances in networking application capabilities are allowing for the electronic exchange of information between computer systems under a point-to-point protocol.

These business objectives are further refined into the requirements of the JIN telecommunications infrastructure, which are:

- Support the exchange of both data and images between all criminal justice entities.

  The basic requirement of JIN is to provide the capability to exchange information between all criminal justice entities in the state using a common standards-based infrastructure. Communications should be handled on a peer-to-peer basis and should not be predicated on routing all requests or information through a central point. The architecture should facilitate moving information:

  » Within a local criminal justice community, such as a county.

  » Between local criminal justice communities (e.g., across the state).

  » Between a local criminal justice entity and state agencies.

- Support information exchanges between systems implemented in a variety of technical environments.

  Implementation should be able to support multiple types of hardware and operating systems and be practical in a variety of programming languages so that organizations can participate.

- Support the immediate transfer of single transactions and file transfers of multiple transactions.

  In addition to supporting messages containing a single transaction, the design should allow a message to contain multiple transactions. The design should also allow for batch file transfer

of large numbers of non-time-critical transactions and for movement of non-transaction-oriented data files.

- Allow coexistence with the existing technical environment that supports information exchanges.

  The new design must allow for continued operation of the existing networks and any other implemented interfaces developed for the exchange of information. This will allow the criminal justice community to retain its significant investment in the technology base that currently exists, while allowing for alternative implementation of the new network and applications and a phased, controlled migration to it.

- Support evolutionary growth as new requirements are recognized.

  The design must be able to migrate or grow over time as new requirements are identified and defined. This includes support of the process of introducing new extensions and software releases into existing operational environments.

- Be built upon existing production industry-standard protocols and open systems technology.

  The design must be based upon current and developing industry standards to ensure compatibility with future technology. This includes the underlying networking environment, as well as the application software and operating systems.

- Provide performance that meets the operational requirements of the criminal justice community.

  If JIN is to support the criminal justice community, it must be reliable and responsive. First, it will be reliable. The goal for JIN is that critical, 24-hour-per-day functions will always be available for use. Less-critical applications will be available when they are needed. In addition, JIN will provide for the reliable transfer of information, ensuring that deliveries are made completely and as directed.

  Second, JIN will meet the response requirements of each business function it supports. It is anticipated that these requirements will vary from function to function. JIN will transfer information and respond to inquiries with the speed required by the business function being supported.

- Utilize existing and future statewide purchased resources.

  To the extent possible, these services should be accomplished through the use of purchased services, such as those being developed by DIS in cooperation with the private sector to provide services at the level of utility functions.

- Ensure a high degree of security and auditability.

  Given the sensitive nature of criminal justice information, it is necessary that JIN provide a high degree of security and transaction auditability. To accomplish this, JIN will need to address the following aspects of security management:

  » Authentication of users.

  » Authorization of users based on previously defined credentials.

  » The ability to encrypt sensitive information transmitted on unsecured networks.

  » Auditing of JIN transactions.

- Be able to be piloted and implemented today, not tomorrow.

  Actual real-world projects must be able to be designed and implemented using today's technology in order to ensure acceptance by the criminal justice community.

The goals or requirements listed above were major factors in developing the JIN design, but other requirements, that have not been restated here, were factored into the design process. The network's technical requirements to meet the business needs and objectives include:

- Support multiple network protocols (System Network Architecture [SNA], TCP/IP, Internet Packet Exchange [IPX], etc.).
- Provide connectivity to existing county and local agency local area networks (LANs) and MANs.
- Allow integration and transmission of new data types (document images, photographs, fingerprints, etc.).
- Support access to legacy systems using existing protocols.
- Support new client/server application architectures.
- Ensure the capability of meeting data security requirements.

- Meet National Crime Information Center (NCIC) 2000 networking requirements.
- Allow connections to multiple state and local applications and application operating platforms from the same workstations.
- Establish an environment for developing new applications based on Internet-working technology.
- Provide the capability for direct intercounty information exchange.
- Enable multiple methods for accessing existing state mainframe systems.

III. PROJECT OBJECTIVES

III. PROJECT OBJECTIVES

This section presents the objectives, scope, and approach for this project.

A. STUDY OBJECTIVES

The JIN Feasibility Study is one of the steps in the state's process for improving the data quality and timeliness of criminal justice information. The goal of the study was to identify and define the requirements, design, potential costs, and implementation plan required to make this network a reality. Specific project objectives included:

- Determining the interest and willingness of local criminal justice agencies to participate in a shared JIN.
- Identifying the technical readiness of local county infrastructures to connect to a shared JIN.
- Determining the costs and effort required by local jurisdictions to prepare for and connect to a shared JIN.
- Refining the design of the new JIN based upon WAN technologies.
- Defining the security requirements and possible infrastructure required to operate the JIN within the context of the criminal justice environment.
- Assisting the state in defining the management and operational frameworks required to administer the WAN.
- Developing a plan for implementation of the JIN.

The results of these objectives will assist the state in making key decisions regarding migration of the telecommunications infrastructure that supports the criminal justice system.

B. STUDY SCOPE

The scope of the study was limited to replacing the existing DOC, WSP, and OAC-supported locations or sites. OAC-supported sites do not include juvenile or tribal courts, which for the most part have no existing network infrastructure provided by the agency. The existing DOL networks and locations are being combined and replaced with a similar multiprotocol network and could be seamlessly integrated with the rest of the JIN when it is fully implemented.

The project scope includes the costs of implementing a WAN, up to and including the local routers, and the costs of connecting to the WSP and OAC data centers. The project scope does not include the costs of any LAN or terminal servers at a given location, the costs of any new NCIC 2000 terminals for local law enforcement, or any costs associated with reprogramming existing local applications written for the current network protocols.

The project's scope can be defined by the following activities and/or deliverables:

- Developing a structured interview and survey instrument.
- Interviewing criminal justice and technical personnel in each county.
- Surveying additional personnel not included in the interview process.
- Documenting the results from the interviews and survey.
- Defining the JIN network requirements.
- Developing an overall JIN technical design.
- Developing JIN security mechanisms.
- Identifying and documenting the costs and benefits of a JIN.
- Assisting in the development of a framework for managing and operating the new JIN.
- Developing a plan for implementing the JIN.
- Completing a comprehensive feasibility study following DIS guidelines.

C. STUDY APPROACH

This feasibility study process was based upon five primary project components: Agency Location Inventory, County Network Infrastructures, Management and Operations Framework, Cost-Benefit Model, and the DIS-compatible Feasibility Study. These components are defined below, along with the approach used to create them.

1. Agency Location Inventory

The agency location inventory documents the current and potential network connection requirements for each agency included within the scope of the study. It provides the information baseline upon

which cost calculations were developed. This inventory of information was collected via the following tasks:

- Conducting state agency interviews. Information about the current networks and connections were identified during initial state agency interviews.
- Developing a baseline inventory. This was done by collecting data about the current network circuits and lines for each available agency. This information was captured into a common repository.

2. County Network Infrastructures

Using the information collected from the tasks in the agency location inventory, the next project component focused on developing a profile of the network infrastructures within each county. This information was collected via the following tasks:

- Conducting local agency interviews. Using the baseline inventory as a starting point, each chair or another representative of the 39 law and justice councils was contacted to schedule interviews with either the council or individuals selected by the person contacted. During these interviews, information about the current county network environment, as well as information pertaining to the desires of the county relative to this project, was collected and documented.
- Conducting technical telephone interviews. In combination with the local agency interviews, a number of county information services staff members were contacted and interviewed via telephone. This information was combined with that from the local interviews to summarize the current network environments.
- Surveying the counties. The next step in completing the county network infrastructure profile was to survey information services personnel in those counties that were missing information about their networks. APPENDIX B contains a sample of the survey instrument utilized during this task.

3. Management and Operations Framework

The next project component focused on assisting the state with definition of a management and operations framework for the network infrastructure that would meet its needs and requirements.

- Defining network administration categories. This task reviewed network management and operations to develop an outline of these areas of responsibility.
- Identifying roles and responsibilities. This task identified which organization would be responsible for each management and operations area.

4. Cost-Benefit Model

This model was developed by comparing current state criminal justice event volumes against a known model of information exchanges. The resulting model defined the efficiencies and benefits associated with the development and implementation of electronic information exchange capabilities. This component involved the following tasks:

- Identifying criminal justice event volumes. The first step in developing the model was to quantify the magnitude of information exchanged between criminal justice system organizations. This was done by obtaining systemwide volumetric numbers for the primary criminal justice events.
- Developing and running a cost-benefit model. After the event volumes were known, the organizational and technical environment for the state system was defined. A state information exchange inventory was documented that identified what information is commonly exchanged between functional organizations, and the cost-benefit model was calculated based upon a number of cost assumptions.

5. Feasibility Study

The last component of the study was completion of the DIS-compatible feasibility study using information collected from the previous deliverables. This component involved via the following tasks:

- Documenting interview findings. Using the agency location inventory and the county network interviews, significant findings were documented.
- Defining the network architecture. The proposed network architecture was identified and documented as a result of information collected from the interviews and the directions of technology.
- Analyzing alternatives. Using the network architecture and business requirements as a basis, alternatives for meeting the state's needs were identified. For each of the two alternatives, the strengths, weaknesses, and costs were defined and a recommendation developed.

- Developing an implementation plan. The plan for implementing the recommended alternative was defined.
- Assessing project risk. The last task in this component was to develop a project risk assessment and to identify ways to mitigate overall risk.

IV. IMPACTS AND ORGANIZATIONAL EFFECTS

IV. IMPACTS AND ORGANIZATIONAL EFFECTS

Organizations both within and external to the criminal justice community would be directly affected by the deployment and migration to a new multiprotocol network. These impacts vary depending upon the current networking capabilities of an agency, as well as the amount of information access required or data collection performed by the agency.

A. CRIMINAL JUSTICE ORGANIZATIONS

Internal to daily operation of the criminal justice system, the following local, state, and federal agencies would be directly affected by the deployment and migration to a new multiprotocol network:

1. Law Enforcement

Most local, state, and federal law enforcement agencies in Washington utilize A Central Computerized Enforcement Service System (ACCESS) network to submit and retrieve information from the state's criminal justice repositories and federal data sources. This network provides the information technology backbone upon which law enforcement operates and communicates. Agencies that would be affected by replacement of the ACCESS network with a new JIN are:

- WSP (eight district offices and 28 detachments).
- County sheriff's offices.
- Municipal police departments.
- Federal Bureau of Investigation and other federal law enforcement agencies.
- DOC and other organizations operating regional computer networks connected to the ACCESS network.

These organizations connect to the ACCESS network either through a WSP-provided ACCESS terminal or via dedicated telecommunications lines to their own regional computer systems. Implementation of a new network would require replacement of the current ACCESS terminals with new intelligent workstations, such as those capable of meeting the new NCIC 2000 specifications. It would also require upgrade of the operating system and application software in each of the regional computer systems connected via the dedicated lines in order for them to be compatible with the TCP/IP protocol. In addition, this migration would require an upgrade to the WSP ACCESS message switching computer in order for it to be TCP/IP compatible.

While this is a significant impact, some regional systems already want to switch to a standards-based networking protocol, and WSP is upgrading its message switching computer. A multiyear migration toward this protocol would be required to complete this effort.

2. Courts

The state's superior and district courts operate on existing multidrop lines that connect them to the OAC mainframe computer center in Olympia. These courts either operate terminals connected to a controller or have installed LANs with a network gateway:

- Superior courts.
- District courts.
- Juvenile courts.
- Municipal courts.
- Four appellate courts.
- State supreme court.

JIN implementation would require the replacement of most network infrastructure equipment installed in each county court. This is especially true for the superior courts, where only a few LANs have been installed.

3. Corrections

DOC is currently replacing its existing SNA network with a new multiprotocol network for both the state institutions and community corrections offices. The impact of implementing JIN would be minimal to overall operation of the agency's facilities, but would provide an opportunity to better integrate the community corrections offices with the local criminal justice agencies.

4. Licensing

DOL has just completed installing a multiprotocol network for its Vehicle Field Services and Drivers Licensing Services sites. JIN implementation would provide the opportunity for better integration with the rest of the criminal justice community.

B. NON-CRIMINAL JUSTICE ORGANIZATIONS

In addition to the above agencies, the following state and federal agencies would be directly affected by the deployment and migration to a new multiprotocol network:

1. State Agencies

Other state agencies use criminal justice information in completing their duties. Often these uses are for background checks and disqualifications based upon criminal arrests and/or convictions. Some access to these information sources uses the existing networks. These agencies include:

- Department of Social and Health Services.
- Department of Labor and Industries.
- Department of Fish and Wildlife.
- Liquor Control Board.

These agencies will be affected by the network replacement if they have not already implemented a multiprotocol network within their organizations.

2. Federal Agencies

Other non-criminal justice federal agencies (such as the Immigration and Naturalization Service and the Internal Revenue Service) currently use the state's criminal justice systems. Their access to these systems may have to be maintained by the source agency, or the users must change their technology in order to retain access.

V. CURRENT ENVIRONMENT

V. CURRENT ENVIRONMENT

A. INTRODUCTION

The purpose of the JIN Feasibility Study is to evaluate the cost and associated benefits to be derived from consolidated the existing data communications network of Washington State DOC, DOL, DIS, OAC, and WSP. This document describes the existing network facilities for each of these agencies and current technology plans that will have a significant impact on the existing network infrastructure.

In the current technology environment, each state agency noted above utilizes a separate networking infrastructure that provides access to the agency's computing resources. In addition, the agencies that will participate in JIN are in varying stages of a network technology transformation from an architecture based on mainframes, leased lines, and fixed-function terminals to one based on the interconnection of intelligent workstations (often connected to a central data warehouse), frame relay permanent virtual circuits (PVCs), and multiprotocol network routers. In support of this transformation, TCP/IP is taking a more prominent position as a networking protocol. As will be discussed further in the following subsections, each JIN agency is pursuing a networking strategy that will position it to interconnect with other LANs, provide higher-speed connections between sites, and improve the service and functionality that it provides its end users. As the agencies transform their telecommunications infrastructure, they have been careful to maintain existing services, reliability, and access to legacy applications.

The composite technology picture of the JIN agencies is highlighted by the parallel utilization of such LAN interconnecting technologies as TCP/IP and frame relay, SNA to provide access to legacy mainframe systems, and a continued reliance on asynchronous and/or proprietary protocol to meet the specific access requirements of critical applications.

The remainder of this section briefly describes each agency's networks and summarizes the major network-impacting technology initiatives.

B. DEPARTMENT OF INFORMATION SERVICES

The Telecommunications Service Division of the DIS administers most voice and data communication lines within the state. Specifically, DIS is responsible for the State Controlled Area Network (SCAN) voice communications infrastructure, a statewide SNA network, and a multiprotocol router-based network. Both the data and voice networks are built upon the DIS Digital Transport Services (DTS) facility. DTS and the two major data networks are discussed below.

1. Current Network Environment

Digital Transport Services

EXHIBIT I, DIS Digital Transport Services Backbone, which follows this page, illustrates the current DTS infrastructure. DTS offers a high-speed statewide infrastructure for providing inter-LATA (Local Access Transport Area) transport service to state agencies. The existing DTS network consists of eight switches or nodes that are interconnected using leased high-speed facilities (1.5 MBs to 45 MBs). The DTS nodes are distributed to provide access to areas of high population, allow for aggregation of inter-LATA traffic, and furnish redundant paths between sites. The DTS backbone provides a range of communications services including voice (SCAN), video, and data.

DIS does not typically provide transport service directly to end user sites, but relies on the local telephone companies to maintain the local facilities. In support of agencies' needs for data communications services, DTS offers two primary options. An agency can establish point-to-point or multidrop private lines from its user sites via a combination of services from the local telephone company and DTS inter-LATA communications, or DTS can be used to interconnect frame relay networks. If an agency opts to use frame relay, the local telephone company would provide service within the LATA and DIS would act as the interexchange carrier providing inter-LATA frame relay connectivity. It has not been clearly determined whether DIS is more, less, or equal in cost to private vendors providing this service.

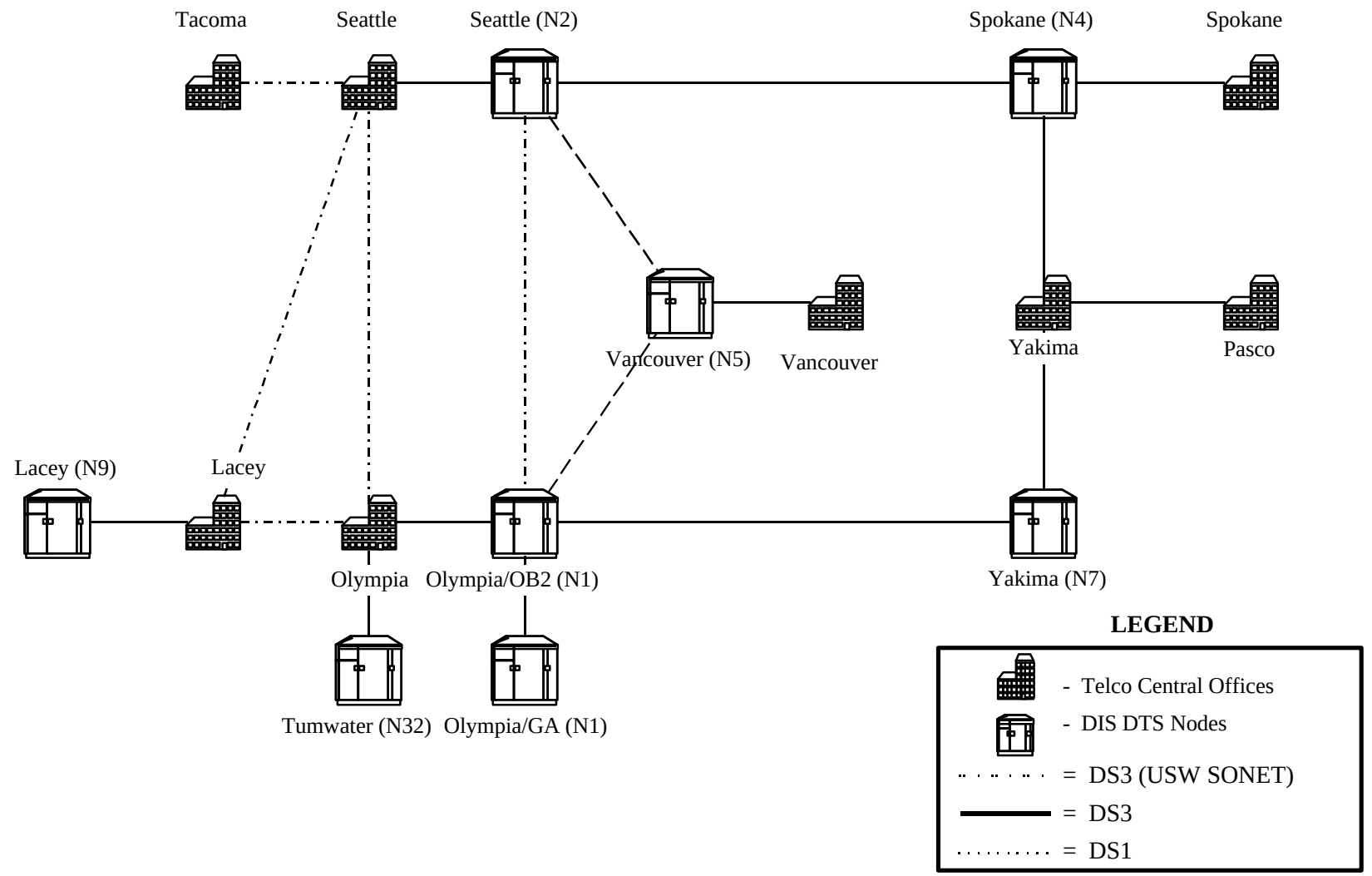
Networks Architectures

In addition to providing the basic transport service described above, DIS manages a statewide SNA network and a multiprotocol routed network. Approximately 34 percent of the traffic on the DTS (described above) is related to the DIS SNA network. An additional 32 percent of the traffic represents data transmitted by other state agencies or information traversing the DIS router-based network.

The DIS SNA network is based on two IBM 3745 front-end processors (FEPs) in Olympia. The 3745s are connected to the DIS mainframe and to other agencies' SNA FEPs, providing cross-domain communication from the DIS SNA network to hosts located on other agencies' networks. DIS also maintains a frame relay-based routed multiprotocol network. DIS provides TCP/IP access to its mainframe from the multiprotocol network. Access to the DAS mainframe is based on operating a TCP/IP protocol stack on the host and providing network connectivity via a channel-attached LAN adapter (IBM 3172 Interconnect Controller).

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
DEPARTMENT OF INFORMATION SERVICES
DIGITAL TRANSPORT SERVICES BACKBONE

EXHIBIT I



ECG MANAGEMENT CONSULTANTS

In the current DIS data communications environment, SNA accounts for 62 percent of all traffic, Uniscope 29 percent, TCP/IP 8 percent, and X.25 1 percent. DIS has projected that by the year 2000, the profile will change, eliminating all Uniscope and X.25 communications and shifting emphasis to TCP/IP. DIS estimates that by 2000, 60 percent of data communication will be TCP/IP and 40 percent will be SNA.

2. Networking Plans and Initiatives

DIS plans to continue to expand and enhance the DTS backbone in response to increased demand and in anticipation of new services such as widespread Internet access, digital imaging, and potentially the widespread transmission of video. Two major DTS enhancements are being considered by DIS at this time: upgrading backbone facilities to Synchronous Optical Network (SONET) and implementing asynchronous transfer mode (ATM) communications. The most imminent DTS upgrade is the migration of existing internodal trunks from DS-3 service to SONET to improve overall reliability. Implementation of the ATM communication infrastructure in the next 12 to 18 months will be based on the availability and cost of products and services and the needs of the client community.

DIS is also focusing attention on the statewide router network. As a result of DIS's project noted above, the composition of network traffic will shift dramatically to increased utilization of the TCP/IP protocol. In support of this change in network emphasis and the desire of many state agencies to utilize the Internet, DIS has been evaluating the existing security structure of the routed network. DIS is preparing to implement a multitier series of Internet "firewalls" to provide varying levels of access from the Internet to information and systems managed by state agencies.

C. DEPARTMENT OF CORRECTIONS

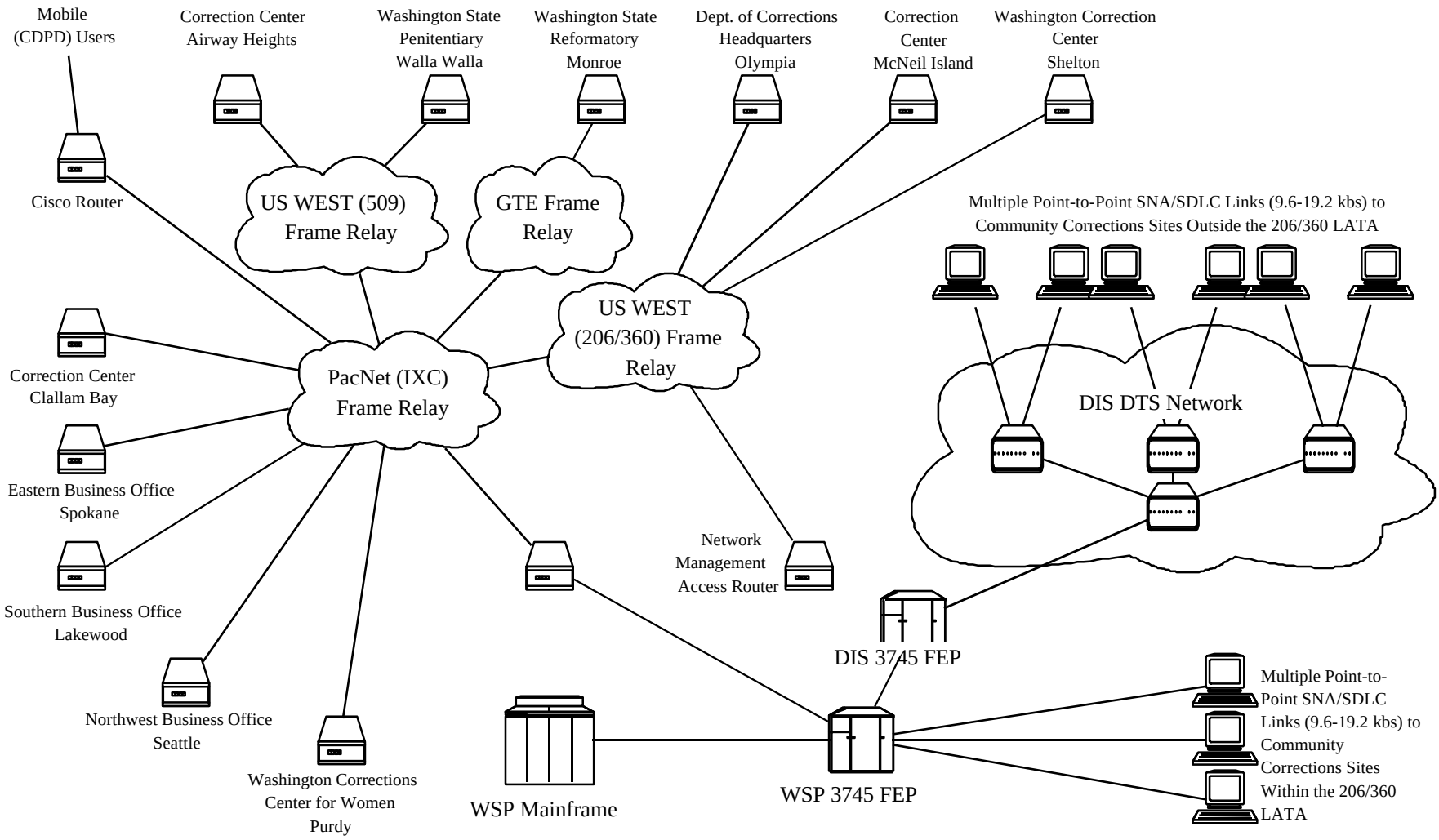
1. Current Network Environment

As illustrated by EXHIBIT II, DOC Current Network Configuration, which follows this page, DOC maintains two parallel networks: an SNA network based on leased lines and a frame relay network utilizing Hypercom routers. The primary purpose of both networks is to provide access from fixed-function terminals to mainframe-based applications operating in the DIS and WSP data centers. The frame relay router-based network was developed in response to a new application that required access to a Unix host using the TCP/IP protocol.

The SNA network operated by DOC is based on point-to-point and multidrop leased lines between the end users' sites and the DIS and WSP data centers. Service to user locations within the 206/360 LATA is provided by the local telephone companies, and the lines terminate on WSP's 3745 FEP.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
DEPARTMENT OF CORRECTIONS
CURRENT NETWORK CONFIGURATION

EXHIBIT II



NOTE: All routers, unless specifically noted, are Hypercom devices.

For users outside the 206/360 LATA, access is provided using DIS DTS (as described above) and the lines terminate on the DIS 3745 FEP.

The frame relay network is based upon Hypercom routers and provides native SNA access to legacy systems and a foundation for implementation of a new system operating on a Unix host. The frame relay network is composed of four interconnected networks (frame relay clouds) that are managed by PacNet, an interexchange services reseller. The frame relay PVCs terminate on a Hypercom router in the WSP data center. The router is then connected to the WSP 3745 to afford access to the mainframe applications. Hypercom utilizes a proprietary router-to-router protocol to enable SNA information to transit the network in its native form. This approach is similar to data link switching and tunneling, but is not based on a predefined and open standard.

Most DOC sites have maintained their reliance on fixed-function terminals and cluster control units. In addition, many sites have implemented LANs for administrative purposes. DOC also provides remote/mobile access using Cellular Digital Packet Data (CDPD) service from AT&T Wireless. The CDPD sites tie into a Cisco router attached to the frame relay network providing access to DOC legacy systems.

2. Networking Plans and Initiatives

DOC has recently completed installation of the Hypercom router network that supports SNA and TCP/IP communications. The DOC Division of Prisons currently plans to have LANs installed in most of its facilities within a year. Through this migration period, it will continue to maintain some existing fixed-function terminals and cluster control units over the next 3 to 4 years. The Division of Community Corrections will implement LANs in its larger facilities, but there are no plans at this time to implement LANs in all Community Corrections sites. DOC intends to replace Community Corrections' fixed-function terminals with PCs and use peer-to-peer connectivity to migrate to the newer technology within a year. DOC also plans to transfer network termination from WSP to DIS before July 1, 1997, using its own routers and channel attachments to the DIS mainframe. This is preparation for transferring DOC processing presently performed at WSP to DIS.

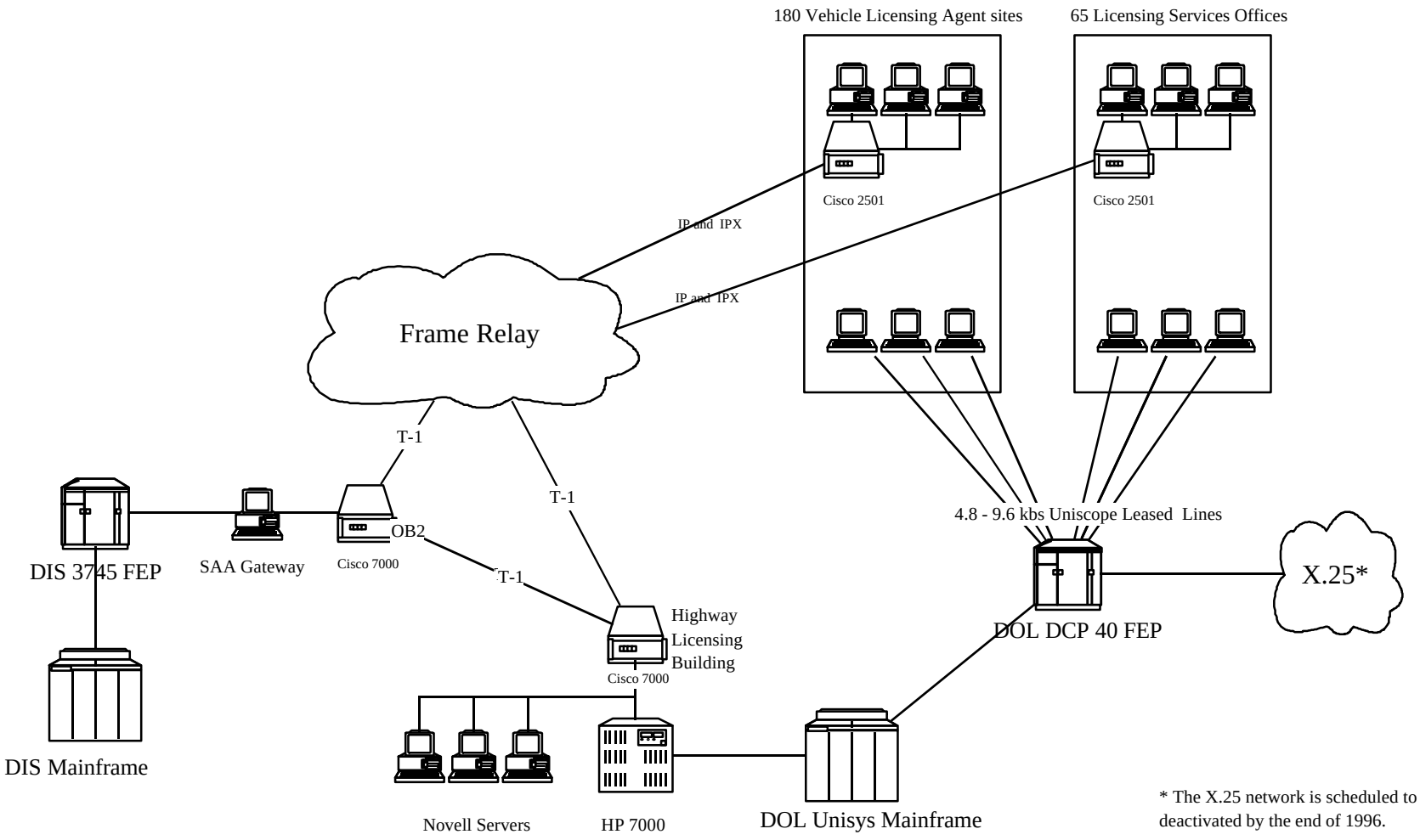
D. DEPARTMENT OF LICENSING

1. Current Network Environment

As presented in EXHIBIT III, DOL Current Network Configuration, which follows this page, DOL maintains two primary networks: a Uniscope network and a multiprotocol frame relay routed network. In addition, DOL maintains an X.25 network that is scheduled for retirement at the end of

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
DEPARTMENT OF LICENSING
CURRENT NETWORK CONFIGURATION

EXHIBIT III



* The X.25 network is scheduled to be deactivated by the end of 1996.

ECG MANAGEMENT CONSULTANTS

1996. The network provides access to DOL's Unisys mainframe, an HP7000 server, and the DIS mainframe.

The multiprotocol frame relay network provides access to both the HP7000 server and the DIS 3745. Each of DOL's 180 vehicle licensing agent sites and 65 licensing services offices is connected to the frame relay network using a low-end Cisco router. Frame relay PVCs provide access to the HP7000 in the Highway Licensing Building and a System Application Architecture (SAA) gateway at the DIS data center. The SAA gateway acts as a protocol converter between SNA and Novell IPX. DOL is transporting both TCP/IP and Novell IPX over its routed network.

The Uniscope network is based on 4.8 and 9.6 kilobytes per second (kbs) leased lines that terminate on the DOL Unisys DCP 40 FEP. The end users of this system are located in the department's 180 vehicle licensing agent sites and the 65 licensing services offices across the state.

2. Networking Plans and Initiatives

The networking initiative currently under way at DOL is closely related to implementation of the Licensing Application Migration Project (LAMP). As noted earlier, the existing X.25 network is scheduled to be deactivated before the end of 1996. When it is deactivated, users of the X.25 network will migrate their access to the DOL routed network. Further development and enhancement of the router/frame relay network will be implemented based on the demands of the new LAMP system.

E. OFFICE OF THE ADMINISTRATOR FOR THE COURTS

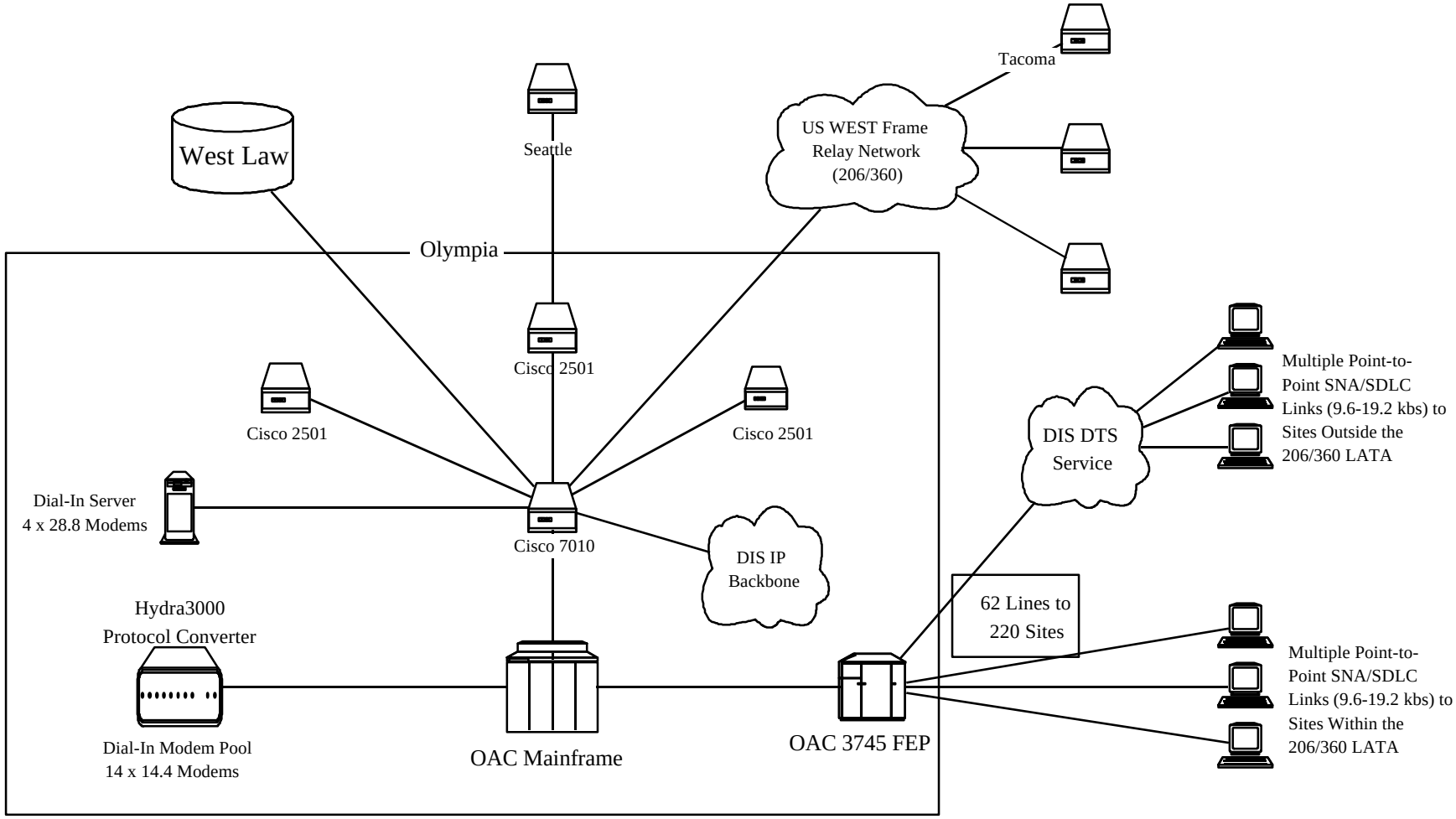
1. Current Network Environment

As presented in EXHIBIT IV, OAC Current Network Configuration, which follows this page, OAC operates two networks to provide access to its Amdahl mainframe applications. There is an SNA network based on multidrop and point-to-point leased lines and a 3745 FEP; and a routed network based on Cisco routers, leased lines, and frame relay services. Mainframe connectivity from the SNA network is through the IBM 3745 and Virtual Telecommunications Access Method running on the mainframe. Mainframe access from the TCP/IP network is based on the use of TCP/IP running on the host and a channel-attached Cisco router utilizing a Channel Interface Processor adapter.

The SNA network consists of 62 lines to 220 sites. OAC provides service for its users located within the 206/360 LATA utilizing facilities leased directly from the local telephone companies; for locations outside the 206/360 LATA, DIS DTS is used as the interexchange facility. The routed network is based on TCP/IP and provides access to a number of sites within the 206/360 LATA. In addition, the

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
OFFICE OF THE ADMINISTRATOR FOR THE COURTS
CURRENT NETWORK CONFIGURATION

EXHIBIT IV



ECG MANAGEMENT CONSULTANTS

network affords access to WestLaw reference service. OAC provides two dial-in access services. One service is based on a Hydra 3000 protocol converter, which provides direct access to the OAC mainframe. The other service facility is based on dial-up access to a terminal server that provides access through the TCP/IP network.

2. Networking Plans and Initiatives

OAC has recently implemented a router/frame relay network and continues to grow this facility. OAC plans to continue to maintain and, as appropriate, expand both the SNA and TCP/IP networks. In addition, OAC is exploring a small number of application pilots that are based on a client/server architecture, and OAC envisions that the client/server applications will utilize the TCP/IP network. The interest in client/server technology has put further pressure for development growth on the TCP/IP network. One of the pilot projects under way involves migrating data currently stored on the OAC mainframe to a Windows NT server for use as a data warehouse, while the other pilot will provide courts direct access to WSP data.

F. WASHINGTON STATE PATROL

1. Current Network Environment

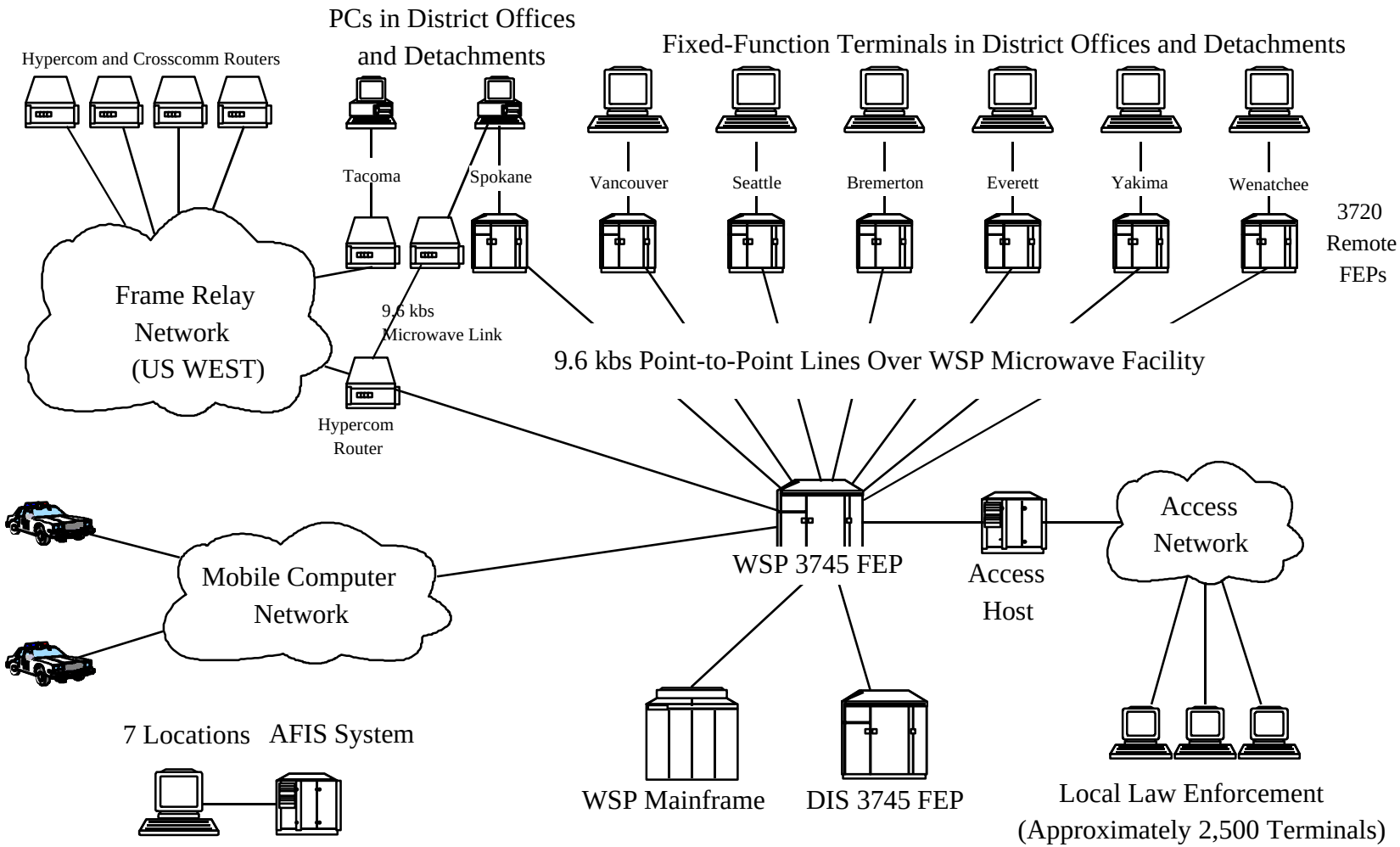
As presented in EXHIBIT V, WSP Current Network Configuration, which follows this page, WSP supports a number of communications networks that provide information access for WSP staff, state agencies, and other law enforcement organizations. The ACCESS network affords local law enforcement and other states connectivity to information managed by WSP and other state agencies, such as DOL. The Automated Fingerprint Identification System (AFIS) network provides crime labs dedicated access to the AFIS operated by WSP. In addition, WSP maintains an SNA network to provide access to its mainframe-based systems and has recently implemented a frame relay-based routed multiprotocol network.

The ACCESS telecommunications system and network is a statewide computerized message switching and telecommunication system through which criminal justice agencies can exchange information of mutual concern within the state and across the nation. ACCESS consists of a central computer and a network of 486 terminals and 26 computer information systems that are connected via leased lines. The central computer is dedicated to switching messages throughout the network.

The SNA network is based on WSP's 3745 FEP, which is connected to the mainframe and also to the DIS 3745, providing cross-domain access to applications and data on other agencies' mainframes. The SNA network is made up of remote 3720 FEPs in each of WSP's seven district offices. The

STATE OF WASHINGTON
JUSTICE INFORMATION SYSTEM
WASHINGTON STATE PATROL
CURRENT NETWORK CONFIGURATION

EXHIBIT V



ECG MANAGEMENT CONSULTANTS

3720s consolidate traffic from the detachment offices and are connected to the central 3745 using point-to-point 9.6 kbs leased lines. It should be noted that many of the WSP leased lines that connect the detachments to the district offices and the district offices to the central 3745 utilize the existing WSP microwave communications facility.

WSP has implemented a frame relay router-based network utilizing Hypercom and Crosscom routers. The router network is currently transporting TCP/IP and IPX. The network's primary purpose is to provide interconnection for office automation needs. In addition, WSP has installed TCP/IP on the mainframe and utilizes a channel-attached Interlink 3672 interconnect controller to connect its mainframe to the Token Ring network. The 3672 is the functional equivalent of the IBM 3172s used by DIS. Utilizing this infrastructure, it is WSP's intent to migrate the remaining district offices from SNA onto the router network.

2. Networking Plans and Initiatives

A number of major technology-related initiatives are in process at WSP that will affect the network and act as the catalyst for change. WSP will continue with its current initiative to migrate the district and detachment offices from their existing SNA facility over to a routed/frame relay facility. This will provide access to legacy systems and will enable other applications, such as office automation, electronic mail, and new core applications based on client/server technology.

Major application initiatives that will have a direct impact on WSP include:

- Mobile Computer Network
- Collision Records and Statistical History
- Fire Department Survey
- Case Management/Investigation Tools

In addition, WSP is exploring the use of new technologies that will further affect the network in terms of bandwidth requirements and protocols. These new technologies include:

- Digital imaging.
- Work flow management.
- Remote network access.
- Telecommuting.

G. DATA CENTER NETWORK CONFIGURATION

Access to the data center mainframes will be based on extending the TCP/IP network to include the mainframes in the DIS, OAC, and WSP data centers. At this time, the DIS, WSP, and OAC mainframes have TCP/IP installed and are operating in a mode similar to that proposed by JIN. As illustrated below in FIGURE 1, Standard Data Center Network Configuration, a router or other channel-attached LAN adapter, such as the IBM 3172 or Interlink 3672 interconnect controller, will act as the interface to the mainframe systems. The 3172s or 3672 will connect to the mainframe and a local data center LAN. This data center LAN will act as the connectivity point for these devices to the WAN. The channel-attached router configuration will have direct access to the WAN and may also be connected to other existing LANs and routers within the data center. The mainframe will run a TCP/IP stack, which will provide access to legacy 3270 applications using TN3270 terminal emulation. The mainframe will also provide a wide range of other host-based services utilizing standard Internet protocols, such as file transfers utilizing the file transfer protocol (FTP) protocol.

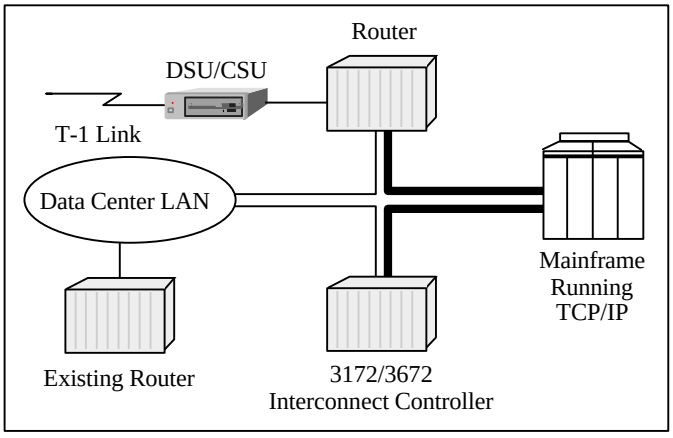


FIGURE 1: Standard Data Center Network Configuration

As noted earlier, the DIS, WSP, and OAC data centers have implemented mainframe-based TCP/IP technology similar to that proposed for JIN. OAC has adopted an approach based on attaching its mainframe to a Cisco router, while DIS and WSP have utilized interconnect controllers (3172 and 3672) that are attached to both the mainframe and the data center LAN.

H. DATA CENTER CONNECTIVITY FINDINGS

Based on a review of the current technology environment and the desired JIN data center architecture, the following observations can be made related to changes required in the DIS, WSP, and OAC data center environments.

1. DIS, WSP, and OAC Have Implemented the Basic Host Connectivity Required by JIN

As previously noted, the DIS, WSP, and OAC data centers have implemented host connectivity solutions that are consistent with the direction specified for JIN. All the data centers currently provide connectivity to the state WAN and have implemented hardware/software solutions that will enable native TCP/IP access to the mainframe environments. Given progress in implementing this technology, there is no immediate need for additional hardware or software to position the three data centers to meet the requirements of JIN.

2. No Standard Configuration is Utilized for Providing Host Connectivity

Though DIS, WSP, and OAC have adopted the basic host connectivity and data enhancements required to support the proposed JIN technology environment, there is no uniform approach to implementing this service. DIS and WSP have implemented a solution using host-based TCP/IP and interconnect controllers, while OAC has implemented channel-attached routers to interface with its host TCP/IP product. The different approaches to providing host connectivity do not in and of themselves present an immediate problem from a JIN perspective, but may represent an additional operational and support requirement in the future.

3. The Capacity of the Existing Host Access Configuration to Meet Future JIN Requirements Has Not Been Established

The initial implementation of TCP/IP on the host, and the WAN connectivity components in the data centers, are adequate to meet the current needs of the individual. It should be noted that the additional network and host traffic associated with implementing JIN has not been fully defined, and as such the impact on the existing data center infrastructure has not been evaluated. Implementation of mainframe-based TCP/IP will create an increased work load on the mainframe, as several teleprocessing functions will now be completed on the host. This increased host work load may become more pronounced as the overall number of TCP/IP sessions to the mainframe increases. In addition, the level of redundancy required for JIN beyond the existing configurations has not been established.

VI. INTERVIEW FINDINGS

VI. INTERVIEW FINDINGS

Presented below are the significant findings derived from the numerous interviews with state and local jurisdictions. These findings are summarized in the first section and provided in detail in the second section.

A. SUMMARY

The basic premise of a shared JIN that provides increased access to criminal justice information is universally accepted. Based upon the interviews, counties support the migration to an integrated JIN based upon a central POP concept. Each state criminal justice agency (WSP, DOC, and OAC) has already begun implementation of router-based networks and are supportive of network integration.

B. DETAILED FINDINGS

The detailed findings that led to the summary presented above are outlined below.

1. The majority of criminal justice functions and activities operate based on a county orientation.

The law enforcement, prosecution, adjudication, and correctional supervision functions of the criminal justice system operate within the confines of the county boundaries. These boundaries dictate that most information sharing and access is between agencies in the same county. The state and federal repositories provide the capability to identify and access information between cities, counties, and states.

2. Many counties are working toward the integration of local agencies via a shared telecommunications infrastructure.

Many counties within the state have implemented their own WANs. These networks have been implemented to facilitate information sharing between agencies within each county. Counties that have implemented WANs include Pierce, Skagit, Spokane, Snohomish, Lewis, and Yakima. Counties that are in the process of implementing WANs include Clallam, Island, and King.

These county WANs include dispatch centers, police departments, courts, sheriff's offices, and prosecuting attorneys. Often WAN implementation is facilitated by collocation of the agencies in a county campus.

3. The E911 funding has assisted a number of small counties to implement improved network infrastructures.

The tax on telephone lines enacted by the legislature has provided significant funding to small counties within the state to implement E911 capabilities. Often included with these capabilities is the implementation of a central dispatch center and records management system. Some counties have used this funding to provide telecommunications connectivity to rural police departments. These new network lines can provide the basis of a county WAN with few enhancements.

Over 15 counties have purchased the Spillman E911 and records management systems. These counties include Pacific, Adams, Lewis, Ferry, and Lincoln.

4. DIS, WSP/DOC, and OAC have implemented the basic host connectivity required by the JIN.

Over the last 2 years, all state criminal justice agencies have purchased and installed the software and hardware required to provide access via a TCP/IP routed network. While no standard configuration is utilized for providing host connectivity, JIN access can be provided to the existing applications.

5. Almost half of the criminal justice agency locations have a WAN connection available at their facility, but only 27 percent are actually connected.

The agency location inventory included with this feasibility study demonstrated that 556 of the 1,215 agency locations (45.76 percent) have a WAN connection available on-site, but only 331 (27.24 percent) are actually connected. Discounting DOL network connections, since all of them are WAN-connected, only 306 of the 965 criminal justice agency locations have WAN availability, and only 81 are actually connected.

6. Current and planned county networks serve only some of the state and/or criminal justice agencies within a county.

While the new WANs within the counties are providing increased connectivity, some agencies are still not being connected. These agencies include community corrections, remote police departments, and state vehicle licensing facilities. The primary reasons for their exclusion relate to organizational issues and funding.

7. JIN integration into county infrastructures can provide increased access to critical state information.

While the county WANs assist local agencies with increased access to regional information, they do not provide a means for prosecutors, municipal courts, etc., to access state information. This is primarily due to technical incompatibilities related to the networks and applications. Implementation of the JIN would assist in eliminating this hurdle.

8. The state lacks a well-coordinated and -communicated improvement plan.

The counties expressed a lack of understanding regarding the state's direction and plans for implementation of an integrated telecommunications infrastructure. Comments received include:

- The objectives and benefits of the JIN are not universally understood.
- There is no detailed JIN migration or tactical plan to assist county improvement efforts.
- There are no tactical links between agency improvement projects.

9. Network and JIN integration requires migration toward a joint state and county technology support structure.

Implementation of a shared network integration design such as JIN will require a new support layer since it is built upon the network infrastructures being implemented within the counties by the county and city computer departments. County integration efforts will determine architecture within the county and the state connectivity will rely upon the support systems provided by the county, including network security.

10. Criminal justice technology governance is divided between the vertical JIC/Executive Committee structure and the horizontal Law and Justice Councils structure.

Integrated technology planning for criminal justice statewide has been provided primarily by the JIC/Executive Committee governance structure. However, over the last few years implementation of the County Law and Justice Councils has begun to shift technology integration planning to the local level. Since the concepts of JIN integration require horizontal integration, these councils have started planning for the increased expansion of county and city WANs.

11. Counties require a clearly defined technology migration strategy in order to plan effectively.

For the counties to plan for future improvements, they must have an overall migration plan from the state that articulates what steps will be undertaken over a given period of time. This includes activities such as network implementation, equipment replacement, and new application availability.

12. State and local funding strategy must take into account the migration toward county-oriented infrastructure support.

If the shared network environment is to operate successfully in the future, the current funding mechanisms used for capital improvements and operating costs must be revised. These mechanisms do not take into account the role of the county and city infrastructure support departments in providing support for the basic network infrastructure within a county facility.

13. The JIN cost-benefit model for automating information exchanges demonstrates that 2-to-1 savings can be achieved overall by implementing the necessary infrastructure and applications.

This model, included with the feasibility study, transforms known and estimated data into quantified costs and benefits for evaluation of implementation scenarios. The summary results from this model identify that the cost of operating a paperless criminal justice system is half that of the current manual methods. This is based upon replacing the manual methods of exchanging information between organizations (paper documents) with the capability of electronically communicating this information between computer systems.

14. The state Information Services Board (ISB) has determined that the state will develop a single telecommunications infrastructure.

A review of the April 1996 report of the Governor's Telecommunications Police Coordination Task Force and interviews with the chair of the ISB and with the DIS director clearly defined the state's policy regarding the implementation of new or multiple networks. No new networks will be authorized by the ISB, and only existing networks can be upgraded. The ISB's intention is for DIS to operate a single multiagency, multiprotocol network backbone that provides services in a consolidated manner much as the state's SCAN system does. This intention has not been reconciled with RCW 43.105 which says DIS will offer services but agencies are not required to use them.

15. DIS is implementing a multiagency WAN following implementation of the INPHO project.

Over the last 2 years, DIS has worked closely with the Department of Health in implementation of the WAN for INPHO. This project has provided funding for a router-based network connecting each of the counties. The Department of Health has worked with the counties to install the routers so that they become the basis of a shared multiprotocol network infrastructure. The Department of Health (DOH) has operational funding for the new network only through this biennium and is seeking partner agencies to share in the long-term costs. It has not been determined whether using the DIS/DOH network will be more, less or equal in cost to pursuing network services from a private provider.

VII. PROPOSED SOLUTION

VII. PROPOSED SOLUTION

This section presents the conceptual future design of the JIN in terms of the network's architecture and features. The design proposes a possible applications model for the use of this network.

A. NETWORK ARCHITECTURE

The JIN will be a multiprotocol routed network that will provide access and communications services to distributed criminal justice community locations across the Washington State. The purpose of the JIN is to consolidate existing application-specific networks onto a single transport network that will provide a level of connectivity and performance that is comparable to or better than existing networking solutions at comparable cost, and to provide a foundation for the development of additional communications services.

The network consists of three major components: routers, transport services, and host/applications access services. For the purpose of this model, a hierarchy of routers and interconnecting transport services has been developed that focuses on the counties of the state of Washington. The primary transport services used in this model are a combination of DIS and US WEST frame relay services. This model provides an approach to host/applications access based on TCP/IP and TN3270.

The network architecture is outlined in more detail in the subsequent paragraphs and is organized into the following areas:

- Network Topology
- Physical Layer
- Data Link Layer
- Network Protocol Layer
- Legacy Applications Access
- Network Management
- Network Expansion/Scalability

1. Network Topology

As stated earlier, the JIN has been designed as a hierarchical network, with major hubs located in county seats and with Olympia as the central hub of the JIN. Each county hub will connect to the central Olympia site using 768 kbs frame relay PVCs. From the county hub, the JIN will extend to other locations in the county using either frame relay service or dedicated private lines. All satellite sites will have one or more "remote" routers. EXHIBIT VI, Network Architecture, which follows this page, provides a schematic diagram of the network components and their connections.

2. Physical Layer

A choice of media will be available for wide-area communications:

- WSP microwave facilities.
- Leased US WEST facilities within an LATA.
- DIS DTS.

Where possible, building wiring for the LAN and interconnecting LANs should be Category 5 unshielded twisted pair or multimode optical fiber in high-volume sites.

3. Data Link Layer

Frame relay services will provide connectivity between satellite cities and into the county hub routers. In the event that frame relay services are not available in the locations, point-to-point leased lines of at least 19.2 kbs will be installed. The county hubs will be connected to the central Olympia hub using 768 kbs frame relay services.

4. Network Protocol Layer

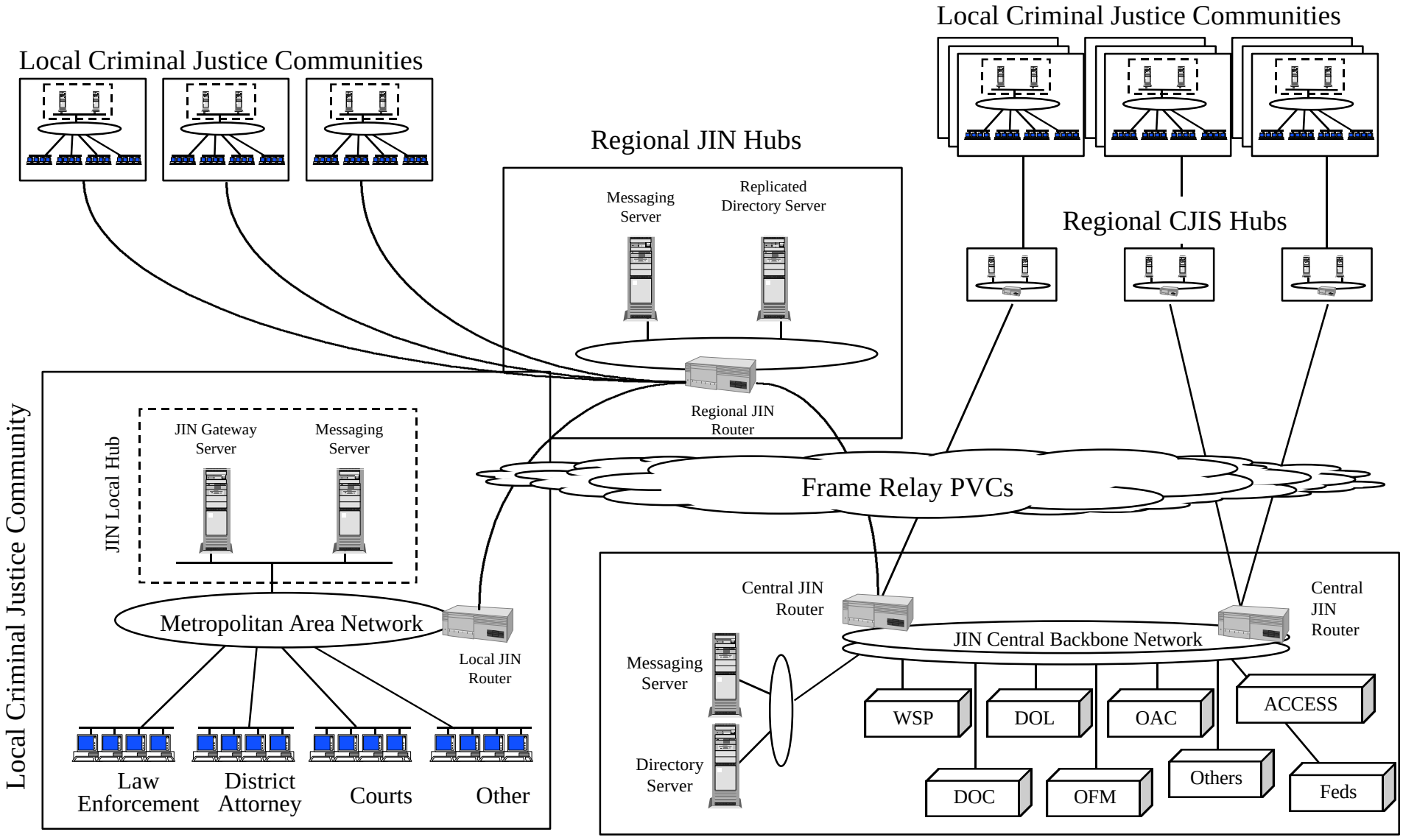
The JIN will be a routed network supporting multiple protocols. Network design will allow for expansion of the set of supported network and transport layer protocols. In its initial implementation, the JIN, at a minimum, will support the following protocols:

- SNA.
- TCP/IP.
- Novell IPX.

EXHIBIT VI

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

NETWORK ARCHITECTURE



ECG MANAGEMENT CONSULTANTS

Network design does not provide for diverse routes between locations, and Olympia is the central hub for all communications. This is an appropriate network design given the current focus on centralized information processing. In this design, the vast majority of network traffic will flow from the counties to Olympia and back to the field. The network architecture will enable direct communications between entities that are in the same county, through the county hub, but all intercounty communications will pass through the central hub in Olympia.

B. NETWORK FEATURES

The features of the multiprotocol network are presented below in terms of legacy application access, network management, and expansion/scalability.

1. Legacy Applications Access

Access to all legacy applications will be via TCP/IP and Telnet/TN3270. The host operating environment will be upgraded to provide host-based TCP/IP services and a LAN attachment from the mainframes to the JIN. The primary advantage of Telnet/TN3270 as the terminal emulation software product is its capability to provide a single solution for access to both SNA and non-SNA applications. EXHIBIT VII, Host Access Components, which follows this page, illustrates the configuration of the components required to provide infrastructure access to legacy systems.

Two potential solutions will be available to end users of the JIN to gain access to legacy applications. The first option is for access from LAN-attached intelligent workstations. In this scenario, end users will install TCP/IP on their LAN-attached workstations and will establish a session with the target applications using TN3270 for 3270 applications and Telnet for other TCP/IP-based applications. If the end user has a fixed-function 3270 terminal, the desired approach would be to replace the existing 3174 cluster control unit with a "gateway" control unit that will support TN3270.

2. Network Management

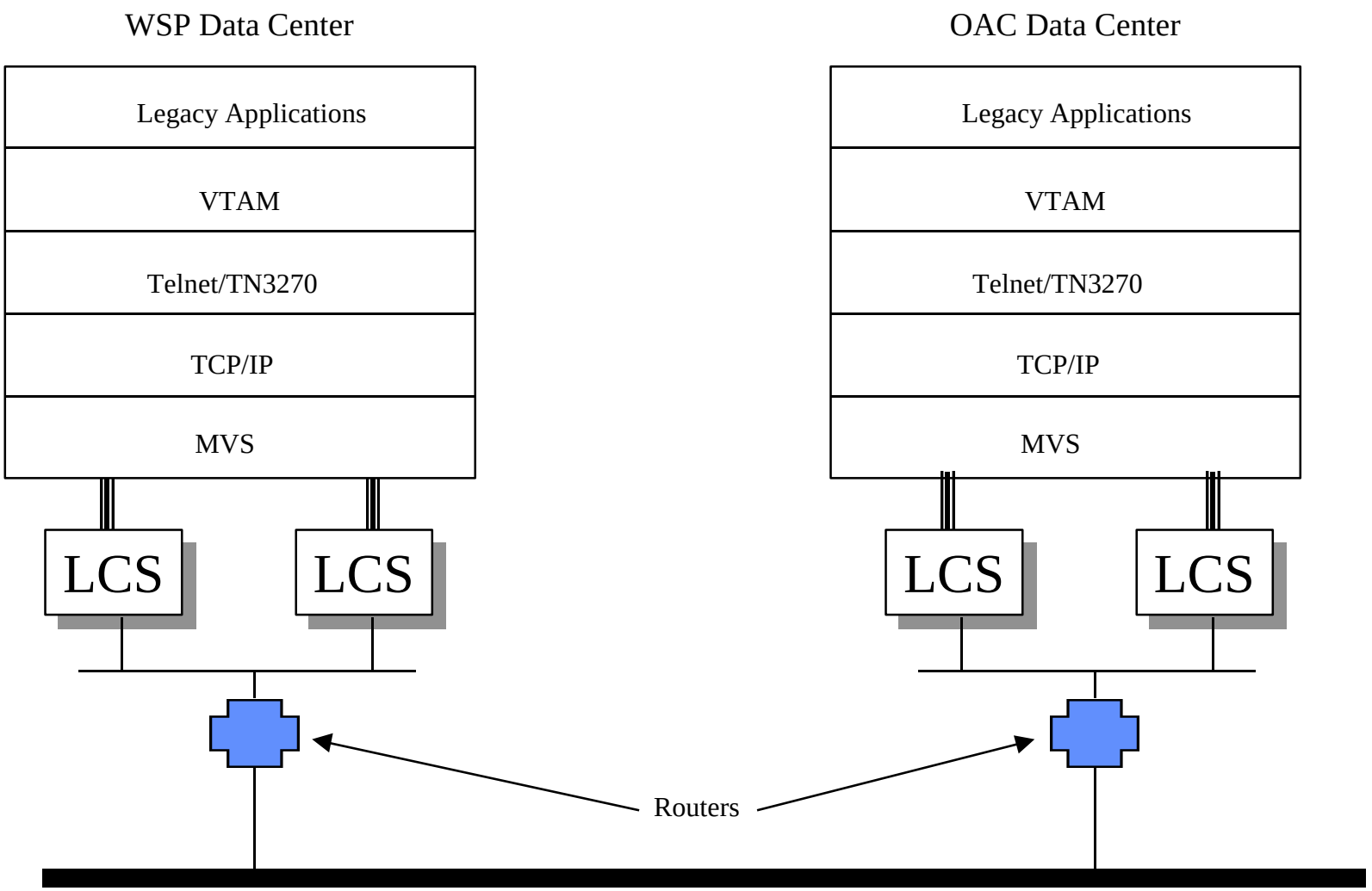
The network management architecture provides a common support foundation for all of the networking components in the JIN. Following is a list of the basic functions that the network management architecture must address:

- Address administration.
- Name/address resolution.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

EXHIBIT VII

HOST ACCESS COMPONENTS



ECG MANAGEMENT CONSULTANTS

- Problem determination/resolution.
- Configuration management.
- Capacity management.

To provide a common network management structure to all of the components that are deployed in constructing the JIN, Simple Network Management Protocol (SNMP) should be the foundation for the network management architecture. All network components will need to provide SNMP agents that support Management Information Base 2 (MIB2) network management variables. The SNMP Manager should be able to automatically parse the MIBs of all network components and generate a graphical representation of the network. The SNMP Managers will provide the platform for the previously outlined network management functionality.

3. Network Expansion/Scalability

A significant feature of the JIN's current design is its ability to adapt to changes in the environment. In the current environment, the majority of network traffic consists of 3270 screen images destined to the central data centers in the Olympia area. Based on existing traffic patterns, 768 kbs PVCs from remote sites to the DIS backbone network in Olympia will meet the current needs of client organizations. As more peer-to-peer distributed computing emerges, the network can be reconfigured and expanded to provide regional network hubs, minimizing the amount of "back hauling" of traffic from Olympia. The size and number of the PVCs that make up the transport components of the network can be expanded to respond to increases in network volume.

C. APPLICATION MODEL

The JIN Application Model describes an application infrastructure that can be utilized to maximize the network's capabilities to meet the overall goals of JIN. When fully deployed, the JIN Application Model is based on a three-tier client/server architecture, composed of a client component providing access to one or more databases and applications from each participating criminal justice agency. Underlying these client/server elements is a messaging system composed of distributed message servers for exchanging messages asynchronously between the JIN Client applications using gateway servers and the JIN data servers or host systems. The Application Model describes the functions performed by each component in the overall application structure.

1. JIN Data

The applications and computer systems supporting the criminal justice system are sources of information to be shared with other organizations. They are defined in the context of this Application Model as JIN Data Servers. They provide information from an organization and make it available to other criminal justice organizations participating in the overall design based on the JIN information standards. Examples of JIN Data Servers using this definition could be the new WACIC and WASIS databases, the DOC Offender-Based Tracking System (OBTS), the Judicial Information System (JIS) data warehouses, and regional systems.

2. JIN Server

As shown in EXHIBIT VIII - JIN Application Model, which follows this page, the JIN Server is the central component in the Application Model. This server provides for administration and control of the JIN and is a logical extension to the current ACCESS state message switch and its functions. The JIN Server, like the current ACCESS message switch, will have a 100 percent availability requirement. The following functions are performed by the JIN Server:

- Message-handling services, including routing and storing JIN transactions.
- Maintaining a directory of addresses and information about JIN organizations.
- Security functions, such as authenticating end users and authorizing them to JIN.
- Auditing and logging all transactions through the JIN Server.
- Constructing JIN messages based on a predefined message format.
- Maintaining indexes to local community and statewide JIN information.
- Maintaining indexes and access paths to national and interstate systems.

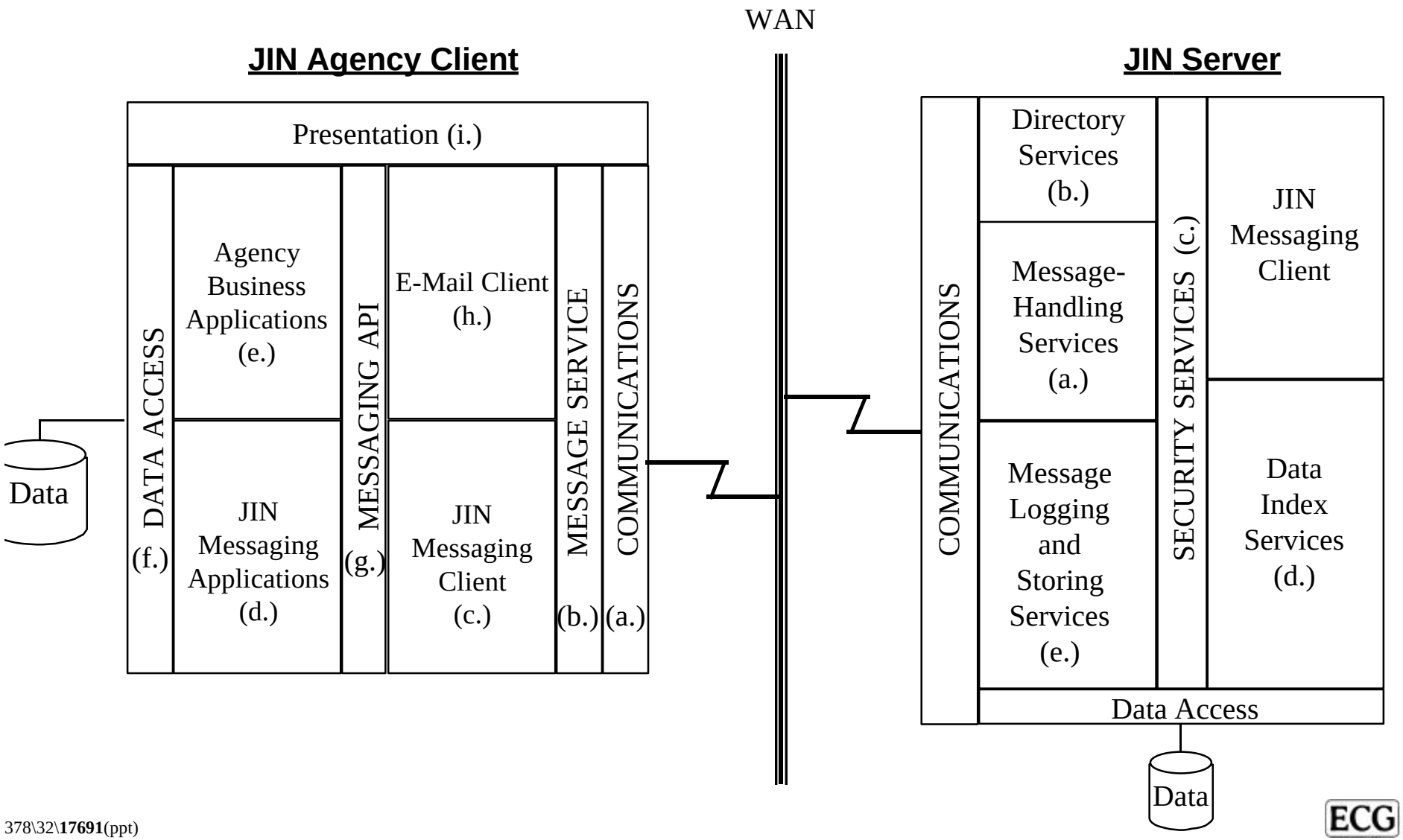
These functions are much like the message-switching functions of Washington's current ACCESS network. However, there are three major differences under this architecture. First, the message-handling services and message formats are based on open standards that extend beyond the criminal justice community. Second, the use of standard messaging services frees the JIN Server from having to maintain a program link with the agency application. Third, the JIN Server may be deployed as either a single central server or as a network of servers serving agencies by geography or political organization (state, county, local).

EXHIBIT VIII illustrates the relationship between an agency computer system or client and the JIN Server, and the major components of each. The JIN Server could operate on a message basis much

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

EXHIBIT VIII

APPLICATION MODEL



ECG MANAGEMENT CONSULTANTS

as an Internet Web server does. All JIN messages could be based on well-defined data structures, described by a set of predefined data exchange formats consistent with the JIN data standards. These messages could use a standard interface to the JIN messaging system and supporting messaging services on the JIN Server for all JIN communications. Based on the client's request, the JIN Server may reconstruct the request in appropriate message format and queue the message to one or more destinations using a standard messaging system interface. Since there are no direct communications between the JIN Server and host system and/or data servers, the messaging system could ensure that JIN messages are delivered to the appropriate JIN Data Servers or agency computer systems, and, if the messages are not immediately deliverable, they could be queued until the destination is available to accept delivery. JIN Data Servers could construct responses to queries or acknowledgments to updates and could forward those messages back to the JIN Server. The JIN Server could correlate one or more response messages and deliver them to the client either in a composite message or as the information arrives from the data servers, depending on the message format and delivery options set by the client when requesting the information. The components of the JIN Server are described below and correspond to the components identified in the exhibit.

a. Messaging-Handling Services (MHS)

Each application component relies on the service of the underlying messaging system to ensure message delivery. The JIN messaging system is similar to an e-mail delivery system, and it would be appropriate to develop the JIN messaging system using existing e-mail standards, such as X.400 or SMTP.

The purpose of the messaging system and MHS is to ensure that information, queries, and acknowledgments are delivered. The messaging system determines the appropriate routing for the transaction and attempts to send it to that destination. If the message cannot be delivered to its destination, it can be either stored or forwarded to an intermediate messaging server, which could guarantee subsequent delivery of the message.

b. Directory Service

As described above in the discussion of the JIN messaging system, the directory is required to define the network address for delivering JIN messages and the network addresses of alternative message servers. Given the requirement for a stable messaging system for the JIN technology architecture, it is necessary to have well-defined and reliable Directory Service. The Directory Service would be based on an accepted standard, either the Internet Domain Name Server (DNS) or the OSI X.500 standard. Implementation of the directory should be highly controlled, as directory errors could create significant problems with system operations. Though it is possible to implement either DNS and X.500 in a distributed manner, implemen-

tation of the JIN Directory Service should be based on a single domain or name space. For performance reasons, it may be necessary to replicate directory information to several directory servers, with a single central site acting as the authoritative information source.

c. Security Services

The JIN Server could evaluate the received messages to authenticate them. The security service component of the server validates the purpose, agency, user, and location. This interrogation could be based on centrally maintained security tables. Based on the results of this validation, the JIN Server could provide the message with credentials that the receiving JIN Client can rely on for authenticity. Network security is discussed further in the next section of this document.

d. Data Index Services

The JIN Server could also provide index services for gaining access to criminal justice information maintained by state and local agencies and for national and interstate systems. The JIN data indices are specialized data sources on the JIN Server that provide information regarding the availability and location of criminal justice data. There could be state indices (such as the incident index) and there could be indices associated with local criminal justice communities (such as a county index of persons of interest). The indices could be accessed using predefined messages and the JIN messaging system. Frequently, index information could be obtained prior to initiating a request to other data servers.

A JIN Client could construct a query to one or more indices regarding a person, vehicle, or other area of interest. In response to these queries, the index servers could build a list of data servers known to have information related to the query subject. This list could be inserted into a JIN message and queued to the messaging system. The JIN Client would be able to utilize the response from the index request to construct queries to one or more data sources known to have information related to the area of interest.

e. Message Logging and Storing Services

In addition to the above application services, the JIN Server could provide for the creation and maintenance of audit trails by message logging. This is similar to the existing ACCESS Switch function in which each message that is routed through a JIN Server could be written to a file for auditing or message recovery.

3. JIN Agency Client

JIN agencies vary in their hardware and software configurations, and this affects the architecture of the software that could be used to access the JIN Server. Some agencies operate host-based systems with terminals; others are operating a client/server environment; while others maintain a combination of the two. Agencies also vary in the applications that they use. Some have advanced and specialized applications, while others have none. It is anticipated that different agencies could subscribe to this architecture at varying rates.

To provide a common understanding of how to provide such varied environments with access to the JIN, an application model of the JIN Agency Client was developed. The JIN Agency Client comprises applications operated by a participating JIN agency that include the agency's existing operational applications, applications that directly support JIN participation, and other key applications supporting such activities as database management and communications.

The Application Model presented previously in EXHIBIT VIII shows the general architecture of the JIN Agency Client. While they may be distributed throughout an agency's computing environment in a manner dependent on the configuration of that environment, the general components of the JIN Agency Client include those described below.

a. Communications

To transmit information between agencies across the JIN, participating agencies must use a common communication application. For JIN, this must support TCP/IP protocol. Such applications are commercially available.

b. Message Service

To interact with the MHS on the JIN Server, a JIN Agency Client must have messaging software that is programmed to submit and receive electronic messages following the standard messaging protocols of SMTP or X.400. Once again, these applications are commercially available.

c. JIN Messaging Client

Between the MHS and any JIN-knowledgeable applications on the JIN Agency Client is the JIN Messaging Client. This software basically functions as an analyzer/dispatcher that reads any outgoing message from the applications and packages the message into the appropriate JIN standard format. The software also reads incoming messages and determines which application should receive and process them.

In client/server technology terminology, the JIN Messaging Client described in this design is a "very thin client." This is done to provide maximum flexibility in selecting operating platforms and deploying the clients. Since the design is based primarily on the capabilities of the JIN Server, it is possible to develop multiple JIN Messaging Clients that can operate on a range of platforms. Since the JIN Messaging Client is a software component, it is possible to run the client and other applications unique to a particular criminal justice community on the same operating platform. In addition, it should be possible to insert the JIN Messaging Client functionality into an existing application to provide a high degree of integration between existing systems and the JIN.

This application is comparable to a more common application that is also shown on EXHIBIT VIII - the E-Mail Client. The E-Mail Client manages electronic messages between persons. The JIN Messaging Client manages messages between application programs. This application would be based on available off-the-shelf software, but would have to be customized to operate for JIN.

d. JIN Messaging Applications

JIN Message Applications are new business applications required to submit and/or receive JIN messages. These programs serve to route data to and from the business applications of the agency. These applications are not commercially available off-the-shelf, but may be programmed by the agency in any major language and can be either on-line or batch programs.

On-line programs could be developed to provide real-time interchange of data. On-line JIN application programs would operate in an interactive fashion with all related applications. These programs could be called by the agency business applications through an application programming interface (API) and accept data for submission to the JIN. The application could provide this information to the JIN Messaging Client and Message Service for submission to JIN. In similar fashion, the on-line JIN Messaging Applications programs could receive data from the JIN Messaging Client through the API and pass this data on to the agency business application.

Batch programs could perform the same functions as the on-line programs. However, the major difference between the two programs is in the method used for sharing data with the agency business application. In a batch mode, data is likely to be shared by updates and accesses of the host system database.

e. Agency Business Applications

These are the applications currently in place that are used by the agency to support operations. Examples include booking systems in local jails or the vehicle registration system maintained by Washington DOL.

f. Data Access

Under the JIN architecture, criminal justice information could be controlled through database management systems. These systems could be used by both the Agency Business Applications and the JIN Messaging Applications. These data access systems should comply with ANSI SQL (1992 or later). Such applications are commercially available .

g. Message Applications Programming Interface

The critical link required to develop JIN Message Applications is the existence of an API that is available to the programming languages in order to talk to the messaging system. Standards available are Messaging API (MAPI) that is being led by Microsoft and the vendor-independent interface being developed by the X.400 API Association (XAPIA). Technically speaking, these specifications are very similar and could converge into one standard within the next few years.

h. E-Mail Client

In parallel with the JIN Messaging Client, an agency could also have a similar e-mail system with a standard e-mail client. Examples of e-mail clients include Microsoft Mail, Lotus cc:mail, etc. These mail clients operate very similarly to the JIN Messaging Client and use the same basic message-handling system and communications. They differ only to the extent that the JIN Messaging Client processes structured data and images, while the e-mail client processes e-mail only in the form of text, images, or other objects.

i. Presentation

The final component of the Application Model for the JIN Agency Client is the presentation component. This component provides the end user interface in the Application Model. Agencies with existing applications have already developed this component for their applications. This component must be developed and implemented for other agencies.

VIII. JIN SECURITY

VIII. JIN SECURITY

The JIN will be called on to perform or support a number of activities that could create security risks for the enterprise systems of JIN participants. However, these activities are essential and give JIN much of its inherent value. These activities include:

- Transmission of confidential information.
- Sharing of data and images between systems via JIN.
- Execution of programs across JIN, including:
  - » Programs that operate remotely on client systems (e.g., Java and Java Script).
  - » Centrally operating programs that access enterprise resources (e.g., Common Gateway Interface [CGI] or other programs providing database access).
- Public access to selected databases connected to the network (e.g., public access to court records or criminal history records).

To support these key activities, JIN must maintain an effective security structure that does not burden participants with undue restrictions, costs, or maintenance requirements. To develop such a structure, it is important to have a clear picture of the risk exposure JIN faces. Once risk exposure is defined, the components of the security structure - hardware, software, policies, and procedures - can be defined. The risk exposure is summarized below, followed by a presentation of the security structure and an estimate of its costs.

A. JIN SECURITY EXPOSURE

JIN has been designed as a private network with access restricted to a limited set of authorized participants. These participants will be certified and recertified on a regular basis. Each certified participant is expected to take steps to maintain network security. However, there will be many participants and network nodes. Some participants may be managing both public access and JIN access and so may be potential points of security weakness for JIN.

1. Areas of Exposure

The areas of exposure are ever-evolving and growing as new methods of compromising networks, hardware, and applications are developed. However, the risk exposure for JIN can be summarized into the following general risk areas:

- Monitoring and interception of information transmitted across the network. Monitoring devices and applications are capable of intercepting transmissions across a network such as JIN. Consequently, monitoring applications can capture host and user authentication data and other sensitive information (e.g., criminal or financial information deemed private by law) as it is transmitted across the network. The authentication data may be used to compromise a host system or application. Likewise, other information gathered in this manner may be used maliciously.

- Transactions with false identity. Another risk for JIN users is that they could receive transactions from an entity purporting to be someone else. A frequently used ploy is an e-mail message from what appears to be a network administrator that requests the recipient to change passwords. This deceptive message could include the network address (IP address), user, and other identifying characteristics and is often referred to as spoofing. Such spoofing tactics can be applied to transactions such as requests for sensitive criminal history information.

- Hostile programs. Hostile programs are applications that repeatedly submit transactions to a server, consuming most or all of that server's available resources. In this manner, the attacking program disables the server.

- Viruses. Viruses are programs that affect the operating system or storage mechanisms of a computer and are spread by sharing data and programs. "Trojan horses" are programs used to deliver applications that can be considered viruses. By accepting a tainted file or program, the computer becomes infected, and the virus establishes itself to take over the computer's operations. In doing so, the virus can replicate itself and do damage. Examples of viruses include:

  - » Polymorphic viruses are viruses that are exchanged while sharing data and that can change their "fingerprint" with each replication (making them difficult to detect).

  - » Trojan horses are apparently-useful applications that also perform malicious activities.

  - » "Hostile applets" are applets (executable code embedded in Web pages that can be run by certain Web browsers) that can compromise a computer.

  - » "Ghostscripts" are similar to hostile applets; however, they are embedded in postscript files and are executed by postscript viewers.

- Terminal hijacking: Terminal hijacking involves using one system as a base from which to compromise other systems. The process is enabled as a system connects to a compromised system as a user device. The hijacking involves the host system taking control of the user system's existing terminal and login connections. Intruders are able to bypass one-time passwords and other authentication methods by tapping the connection after authentication is complete. When this type of activity occurs, the remote site becomes compromised.

JIN security must take into consideration these areas of exposure, as well as the need to secure systems and data available through JIN.

2. Sensitivity of Systems and Data

The second major consideration in developing security for JIN is the sensitivity of the systems and data accessed by JIN. As is the case with security in any arena, one must weigh the cost of security against the cost of loss. An example of this balance could be public information, available at no charge. Such information would require no security against a read-only access.

The security design for JIN is based on the following assumptions about the sensitivity of JIN systems and data:

- The systems of the agencies participating in JIN are highly sensitive and need to be protected from access through JIN. The JIN security design needs to provide the ability to completely block unauthorized access to these systems.
- The resident data of the agencies participating in JIN is also highly sensitive and needs to be protected from modification through JIN. The JIN security design needs to be able to completely block unauthorized modification of this data.
- Only a limited amount of data transmitted across JIN needs to be secured. The majority of data to be transmitted across JIN is of public record. All but a few limited transmissions may be legally shared by other JIN agencies. For example, an estimated 50 percent of DOC transactions contain nondisclosable information, excluding e-mail.

As a result, the focus of security for JIN will be on maintaining the security of each participating system and the databases that each maintains.

B. JIN SECURITY DESIGN

The primary focus of JIN security will be to secure the systems that participate in JIN and the data these systems maintain. The design to provide this security will involve:

- Certification
- Auditing
- Node Architecture
- Authentication
- Node Hygiene

To secure transmissions requiring a high degree of secrecy, encryption will also be available. Each of these provisions is described below.

1. Certification

One of the fundamental steps in securing JIN is to certify the security of each participant. Certification would involve:

- Setting guidelines for personnel and system access to JIN. These guidelines would require JIN to be a closed system and would not allow participating users or systems to act as proxies for external agents.
- Assessing the vulnerabilities/exposure of the JIN participant systems. This would involve identifying all external access points and vulnerabilities in the participating systems.
- Classifying systems to identify the system characteristics, identify the system's security provisions, and assign security levels.
- Classifying users in order to identify the user, ensure that the user subscribes to security procedures, and identify the access privileges of the user.

This certification helps to define and establish the level of trust to be maintained among all JIN participants.

2. Auditing

To help make certification work, audit and recertification programs are needed. This audit process will involve:

- Review of user procedures, logs, and documentation.
- Testing of users.
- Review of system administration procedures, logs, and documentation.
- Analysis of system vulnerability using network scanning tools.

Based on the results of these reviews and tests, both users and systems will be recertified for access to JIN. This certification of each user and system can be used by other users and systems involved in JIN.

3. Node Architecture

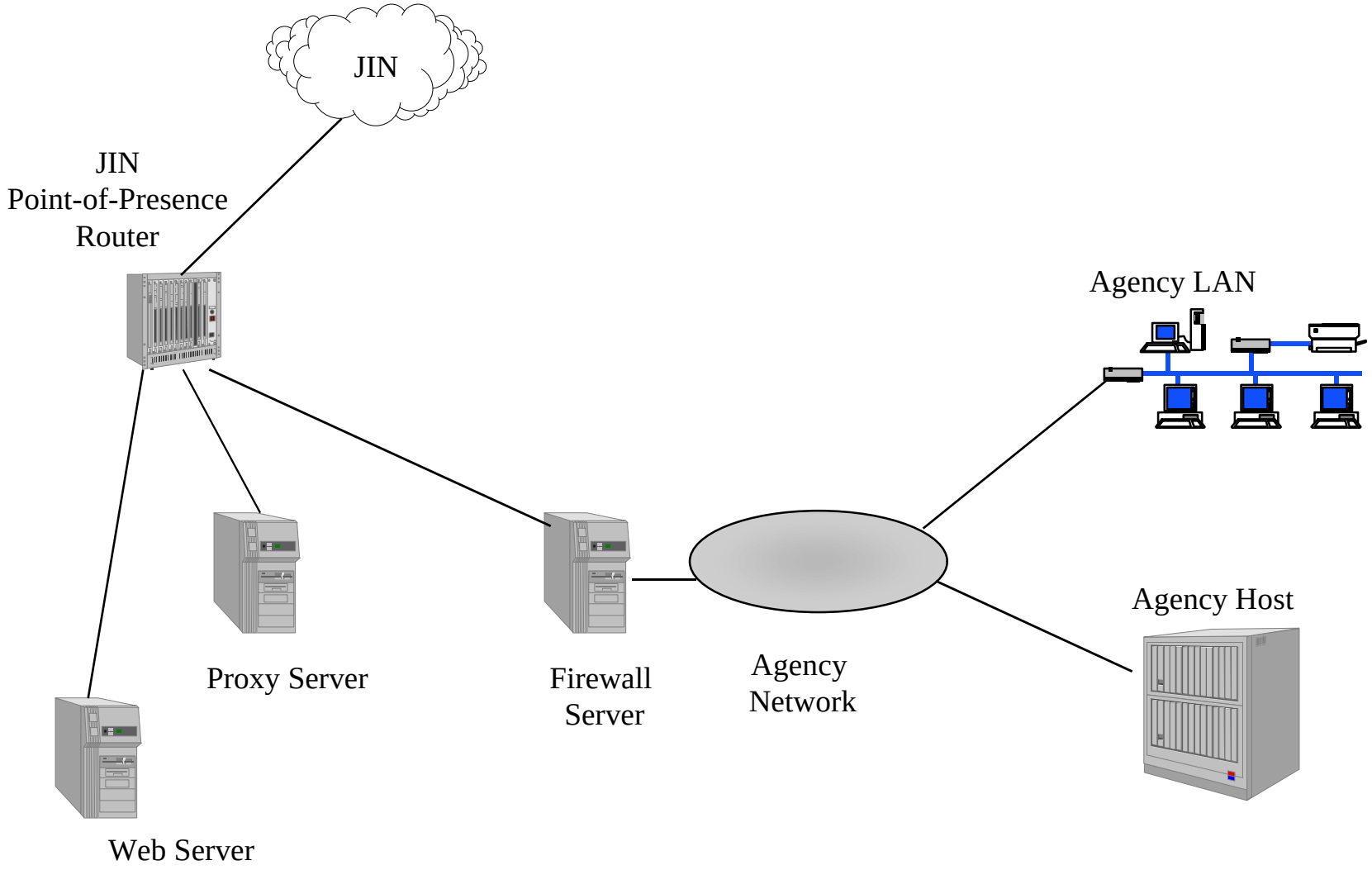
The architecture of each node on JIN may vary, based on the security requirements of the agency using that node. The fundamental assumption for participating in JIN is that at any point in the network, a router may be the only component keeping intruders from JIN. Routers determine how messages from a given address wish to be routed and whether those messages may be routed as requested. Given this assumption and the need to protect agency systems and data, steps must be taken to control access to these systems and data from JIN. The components that can provide this filtering are depicted in EXHIBIT IX, Basic Node Security Architecture, which follows this page. These components include:

- JIN point-of-presence router. This is the router providing access to JIN. Maintained by the subscribing agency, this router restricts the network addresses from which transactions will be accepted by the agency.
- Firewall server. This is a limited-function server that authenticates and filters transactions submitted through JIN to the agency. As its name connotes, this mechanism is a wall between the agency and unauthorized intruders who may have gained access to JIN. This server interrogates each transaction submitted to:
  - » Verify the identity of the submitter.
  - » Determine the authority to submit the transaction.
  - » Log the transaction.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

EXHIBIT IX

BASIC NODE SECURITY ARCHITECTURE



ECG MANAGEMENT CONSULTANTS

- Proxy server. This server resides on the agency side of the firewall. It acts as the proxy and gateway for all transactions out of the agency and provides a single identity and address for the agency in its interactions with other systems. In this manner, external entities cannot gather internal agency identities and addresses.

- Web server. This server resides outside the firewall and provides information from the agency to external entities, such as other JIN participants. This server is periodically populated with data from agency systems and databases. It responds to requests for information from other JIN participants. Because this server resides outside the firewall, it is considered a sacrificial server - a device that could be compromised without affecting mission-critical systems.

EXHIBIT IX shows a basic configuration used to secure an agency computing environment. Many variations of this configuration may be employed to meet the needs of the agency. EXHIBIT X, Multitier Security Architecture, which follows this page, shows a more complex configuration that provides security for both JIN and Internet access. This configuration provides multiple tiers of networks supported by the agency: public (for Internet access), trusted (for JIN access), and private (for agency-only access). As with the basic configuration, the components are used to address the following threats:

- Unauthorized network access: Routers provide the first line of defense, keeping private and trusted networks cloaked from public view.

- False identity: Firewall servers go beyond the network addresses used by routers and use other factors to authenticate the transactions received. Usage of proxy servers limits the ability of intruders to obtain internal, trusted network identities.

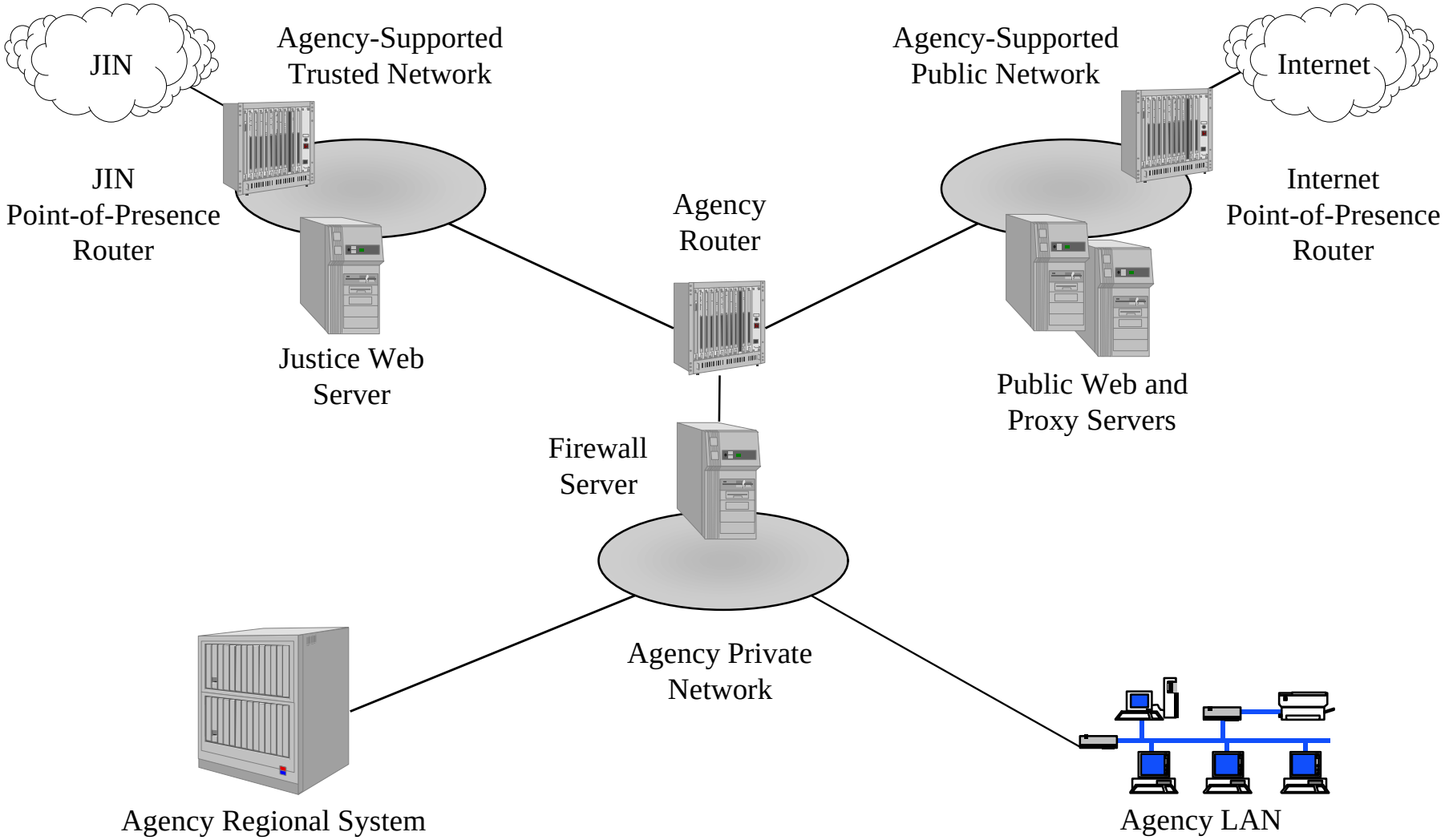
- Viruses: Usage of limited-purpose, firewall, proxy, and Web servers mitigates the impact of viruses. The dedicated nature of the firewall server provides barren ground for the virus to be implanted and shelters the agency from unwanted transactions. Second, the sacrificial Web and proxy servers residing outside the firewall allow automated interaction with other entities without providing access to the internal agency environment.

- Terminal hijacking: The combination of servers and the transaction-based structure of JIN interaction limit the ability to hijack a terminal. Because the interaction uses limited-purpose servers outside the firewall, the internal agency environment is not exposed. Secondly, the use of transaction interchange instead of telnet connections between servers limits the intruder's access to core server functions needed in hijacking.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

EXHIBIT X

MULTITIER SECURITY ARCHITECTURE



ECG MANAGEMENT CONSULTANTS

4. Authentication

User authentication is a major component of the JIN security design. JIN will use application software to identify and classify each user on the network. In this manner, each system on JIN will be able to interrogate any transaction that is received and determine who has submitted it. Then, based on local agency policy, the system can process the transaction based on the authority of the submitting agency.

The authentication process involves administration and transmission security issues. JIN will likely support thousands of users, and administration of user authentication centrally could be difficult. In addition, the data that identifies the source of the transaction must not be subject to interception and forgery.

To administer this authentication in a cost-effective manner, trusted agents will be used at a subnetwork level. These agents will act as proxies for the users they support and will perform the following services:

- Classify and certify users and subagents using JIN standards.
- Maintain certain and consistent security measures (these measures may vary, but they must be consistent and verifiable).
- Act as a proxy for users, submitting transactions to other systems on their behalf.
- Act as a message transfer agent for users, receiving transactions and routing them to intended users.

These agents will participate in periodic audits to verify security and administration procedures. The audits will assess physical and procedural security measures taken, user certification methods, logging, and administrative practices. Based on these audits, the agent will be classified as to the security level maintained, the types of users it supports, the JIN policies it has completely implemented, the agent's network address, and the public key the agent uses. This classification will be maintained and accessible to other JIN participants. Any JIN participant can query and use this assessment to determine how to handle transactions from the agent.

To guard against intruders assuming the identity of a trusted agent, a digital signature may be used. This will be accomplished through public key/private key cryptography.[1] The receiving agent can therefore verify the identity of the sender if required. Digital signature authentication can also be used in establishing telnet or FTP sessions. The signature can be used to authenticate the user.

5. Node Hygiene

One of the key components of maintaining JIN security concerns the maintenance and operating practices of participants. Security designs can be compromised by high-risk practices. To avoid these risks, trusted agents will subscribe to practices that limit exposure to intruders. These practices include:

- Use of servers for a specified purpose. A general-purpose server on an open network is susceptible to compromise. Operating system functions may be accessed more easily by intruders.
- Use of transaction-based interaction. In comparison to telnet and FTP interaction, this tactic greatly limits the activities and authority allowed to external agents.
- CGI limitation. CGI programs allow Web servers to access agency databases to fill a Web page and fulfill an external request. These programs, if not well written, can be used to compromise a system.
- Need-to-know access. All users and applications seeking access to agency data and applications should be granted this access only as needed.
- Page/program control. All Web pages and programs providing information and services to external agents should be reviewed and controlled by a knowledgeable Webmaster or other control point for the agency.
- Virus scanning. All data being accepted by a system should be scanned for viruses.

In a similar manner, client practices can help maintain security. These practices include:

---

[1] Public/private cryptography is based on a relationship between public and private keys such that:

f1 (private key, message) = f2 (public key, message)

To create a digital signature, the sender uses his/her private key (known only to the sender) and the message in a predefined algorithm. The recipient uses the public key (publicly available through a registry) and the message in an algorithm to produce a verifying signature.

- Proxy server use: Use of a proxy server can help maintain the security of internal network addresses and identification.
- Applet and postscript use: Applets can prove to be Trojan horses that can compromise a system. Control and isolation of the use of these features can mitigate the extent of risk.
- Virus scan: As with servers, virus scanning can help identify and correct infections by computer viruses.

6. Encryption

As noted above, encryption will be needed in a limited number of situations for JIN. Due to the public nature and low classification levels of most information that will be transported via JIN, encryption will seldom be needed. In the event that a highly classified transaction is transmitted, it can be encrypted using public key/private key encryption.[2] Such an encryption method requires computer resources and processing time. Therefore, the use of such encryption will be limited to transactions requiring such a high level of security.

C. SECURITY COSTS

The network security design concepts outlined in the previous section can be implemented via a variety of technologies. To determine the range of costs associated with implementation of a security scheme on top of the network infrastructure, a specific set of security technologies must be assumed for the overall enterprise or state. These technologies include security-configured routers, network firewalls, and software token-based authentication systems.

Security-configured routers provide the ability to secure traffic between the county POP and the state network host site. Routers can be configured to turn on data encryption software options in the operating software on router computers. This allows for all network traffic between the remote router and the state hub routers to be encrypted. The cost of the security option in the router operat-

---

[2] This encryption is based on the same relationship between public and private keys. This relationship can be stated as:

f1 (public key, message) = cyphertext and f2 (private key, cyphertext) = message

To effect this encryption, the sender uses the recipient's publicly known key, the message, and the encryption algorithm to create cyphertext. The recipient deciphers the message by using his/her private key, the cyphertext, and a decryption algorithm.

ing systems is assumed to be included is the current system price. Increased costs may be incurred by DIS for administering this option.

Network firewalls limit traffic between the private and public segments of local networks within the counties. It is assumed that only one firewall is required for each of the 39 counties in order to limit traffic in and out of the JIN. Additional open router connections within the county will require additional firewalls. The estimated cost of a firewall for each county varies based upon traffic volumes. The estimated cost of the firewalls is $795,000, calculated based upon the table below.

County Size	Cost/Unit	Number/Units	Total Cost
Small	$15,000	13	$195,000
Medium	20,000	18	360,000
Large	30,000	8	240,000
TOTALS		39	$795,000

Token-based authentication systems are used to ensure that users signing onto the network resource are who they say they are. Hardware-based token systems include time-synchronous solutions, such as Security Dynamics Technologies, Inc.'s SecurID card. This is the technology currently being used by the Department of Health. The cost of this technology is approximately $35 per user.

Software-based token systems are rapidly maturing in the network security market and would probably be easier to manage. Security Dynamics Technologies also has an enterprise-level product called ACE/Secure that provides network-based authentication in a centralized or distributed environment. This provides additional levels of security and allows for a county-centric administration methodology. The cost of this product is approximately $250 per user.

The overall cost of user authentication security is based upon the total number of estimated users in each of the two categories. This is calculated to be $1,320,000, based upon the table below.

Classification	Cost/Unit	Number/Units	Total Cost
Low Security	$ 35	2,000	$ 70,000
Higher Security	$200	2,000	400,000
TOTALS		4,000	$470,000

The overall cost of the security application needs of the criminal justice enterprise is then estimated as a sum of the firewall costs and the authentication costs, or $1,265,000. In addition, administration of these systems is estimated to require two additional staff resources.

IX. IMPLEMENTATION ALTERNATIVES

IX. IMPLEMENTATION ALTERNATIVES

The alternative models for JIN implementation differ primarily only in the amount of network equipment sharing and management control that occurs at the local level. One model maximizes the use of county and city WAN infrastructures while minimizing the amount of control available to any state agency. The other alternative maximizes agency control but minimizes integration with the county infrastructures. The two JIN alternatives are detailed below. For each alternative, the following are presented:

- Strengths
- Weaknesses
- Costs

A description of the methodology by which the alternatives were analyzed and a recommended solution selected follows the discussion of each alternative. Recommendations are presented at the end of this section.

A. MAXIMUM SHARING ALTERNATIVE

EXHIBIT XI, which follows this page, presents a schematic outlining the shared network alternative. This alternative is based upon the fundamental design concept of network connectivity based upon a common state government POP within each county. Local criminal justice agencies would connect to the POP via the existing or future county WANs to access state and federal application and data servers.

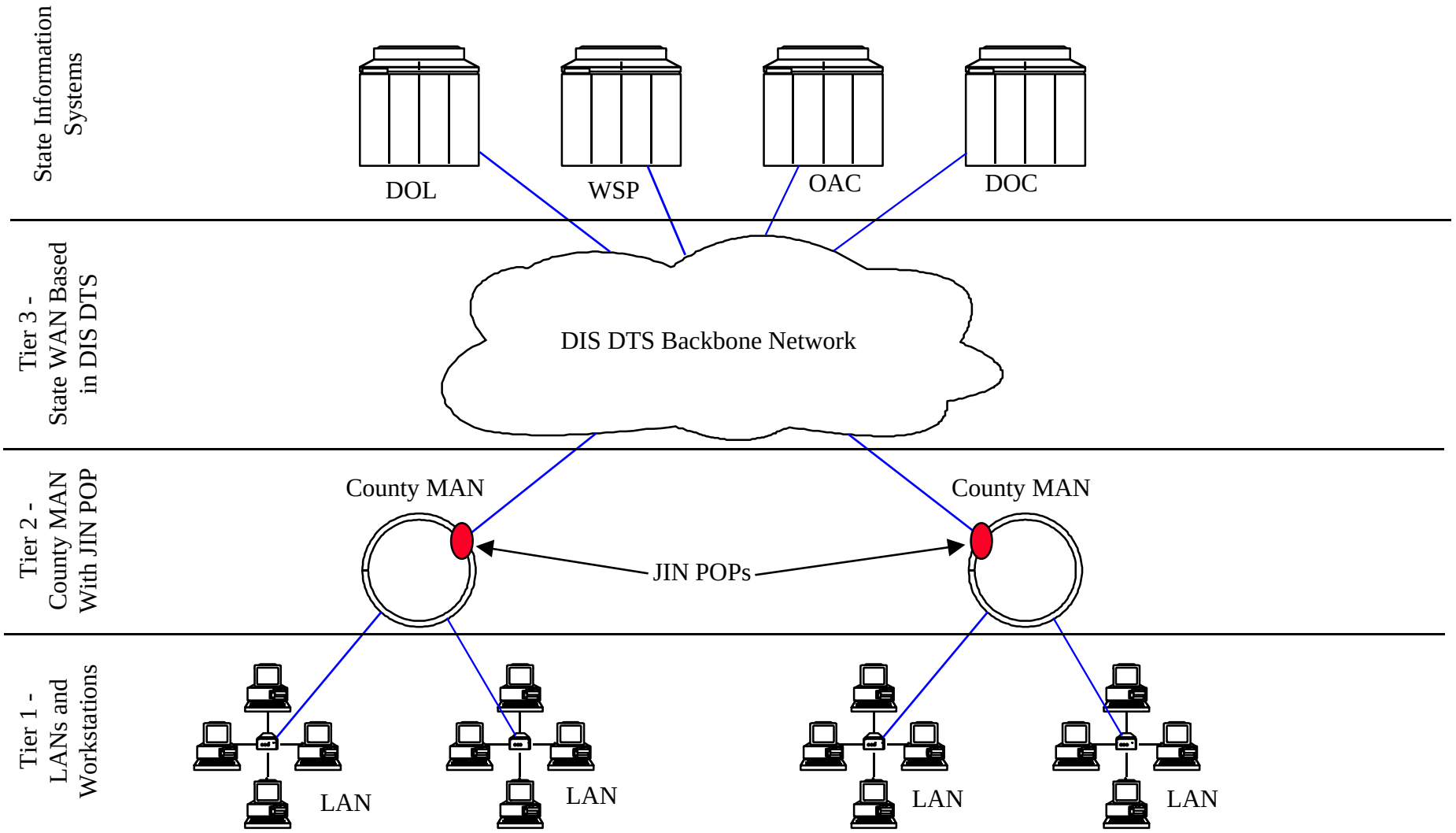
1. Strengths

JIN implementation under a shared model has a number of positive impacts for development, implementation, and operation of the network. This alternative will:

- Meet requirements. The existing network infrastructures do not meet users' requirements for accessing multiple data sources and exchanging new data types. The new multiprotocol network will provide for increased access and data sharing.
- Utilizes county resources. This alternative takes advantage of county network infrastructure and administration that is in place today or will be implemented in the future.

EXHIBIT XI

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
NETWORK SCHEMATIC



ECG MANAGEMENT CONSULTANTS

- Lower complexity for local agencies. The single POP reduces complexity of administration.

2. Weaknesses

There are several negative factors in considering the shared model for JIN. These include:

- Management. Utilization of the county infrastructures distributes management of the network between multiple organizations.
- Control. The sharing of resources between agencies reduces the amount of control available to any given user agency.

3. Costs

EXHIBIT XII, which follows this page, presents the costs associated with implementing the JIN under the maximum sharing alternative for each agency. These estimates include the capital costs of equipment purchase and installation, as well as any line installation costs. Operating costs are calculated by considering the equipment maintenance costs and the line lease costs. The DOL line in the exhibit shows a net cost reduction, since some existing WAN equipment is calculated to be reused and those sites integrated with other agencies. The "No Agency" line in the exhibit is for those criminal justice agencies that were included in the database but currently have no network support by any of the other agencies. These are mostly small police departments, municipal courts, and county attorney offices.

EXHIBIT XIII, which follows EXHIBIT XII, presents the costs of installing the network under the maximum sharing alternative by county. The "Unknown" line in the table represents three small police department agencies for which the appropriate county was not identified.

Equipment costs have been calculated by defining the type of WAN connection required to connect each criminal justice agency location to the JIN. EXHIBIT XIV, which follows EXHIBIT XIII, presents the connection types and their estimated costs. These cost estimates were derived based upon actual setup and maintenance costs incurred by the Department of Health with its INPHO project.

Line costs under this model are based upon the number of users associated with a given agency location. Line lease installation costs were derived from the following formula for calculating the costs per city and from the data maintained in the agency location inventory.

*Installation Costs = Sum (((Workstation Number) * (WAN Utilization Factor)) * $60)*

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

MAXIMUM SHARING ALTERNATIVE COST SUMMARY - BY AGENCY

Agency	Current Month Cost	Current Year Cost	Equipment Install	Equipment Purchase	Equipment Maint./Yr.	Line Install	Line Maint./Yr.	Net Operating/Yr.
DOC	$ 15,849	$ 190,188	$ 51,915	$ 211,800	$ 90,240	$ 22,740	$ 269,520	$ (169,572)
DOL	-	-	(3,840)	(34,304)	(15,312)	-	-	15,312
OAC	32,996	395,952	44,705	184,117	77,110	55,470	653,880	(335,038)
WSP	33,884	406,608	137,525	562,266	238,090	65,550	783,640	(615,122)
No Agency	-	-	188,150	475,540	190,225	34,575	493,360	(683,585)
TOTAL	$ 82,729	$ 992,748	$ 418,455	$ 1,399,419	$ 580,353	$ 178,335	$ 2,200,400	(1,788,005)

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
MAXIMUM SHARING ALTERNATIVE COST SUMMARY - BY COUNTY

County	Current Month Cost	Current Year Cost	Equipment Install	Equipment Purchase	Equipment Maint./Yr	Line Install	Line Maint/Yr.	Net Operating/Yr.
ADAMS	$ 1,489	$ 17,868	3,560	10,412	4,315	$ 1,515	$ 26,320	$ (12,767)
ASOTIN	1,051	12,612	5,080	7,081	2,495	750	15,840	(5,723)
BENTON	1,543	18,516	9,970	50,863	21,515	4,335	54,160	(57,159)
CHELAN	971	11,652	9,210	13,912	5,115	3,285	43,000	(36,463)
CLALLAM	2,505	30,060	9,110	13,455	4,771	3,795	48,560	(23,271)
CLARK	2,216	26,592	13,080	61,275	25,980	6,030	73,680	(73,068)
COLUMBIA	300	3,600	2,980	5,581	2,045	450	9,360	(7,805)
COWLITZ	1,176	14,112	10,055	34,553	14,200	3,195	36,800	(36,888)
DOUGLAS	743	8,916	5,460	10,912	4,065	1,050	17,720	(12,869)
FERRY	402	4,824	3,050	1,750	325	510	10,560	(6,061)
FRANKLIN	902	10,824	9,215	22,310	8,815	2,355	33,040	(31,031)
GARFIELD	300	3,600	4,460	10,412	4,015	720	14,760	(15,175)
GRANT	1,319	15,828	11,560	35,317	14,540	2,355	34,920	(33,632)
GRAYS HARBOR	2,867	34,404	16,150	50,560	20,975	3,855	50,800	(37,371)
ISLAND	1,135	13,620	7,590	16,743	6,585	1,755	21,840	(14,805)
JEFFERSON	1,203	14,436	4,580	6,874	2,476	1,425	17,120	(5,160)
KING	14,343	172,116	53,965	231,705	98,615	40,950	436,800	(363,299)
KITSAP	2,258	27,096	11,710	36,067	15,065	6,600	70,400	(58,369)
KITTITAS	1,206	14,472	10,570	22,367	8,636	3,195	44,400	(38,564)
KLICKITAT	1,173	14,076	6,580	7,831	2,570	1,785	31,440	(19,934)
LEWIS	1,693	20,316	15,230	33,736	13,345	4,110	48,000	(41,029)
LINCOLN	689	8,268	7,590	16,743	6,585	1,035	20,640	(18,957)
MASON	1,429	17,148	5,030	6,831	2,320	3,735	39,840	(25,012)
OKANOGAN	1,534	18,408	12,080	31,486	12,670	2,775	53,400	(47,662)
PACIFIC	1,512	18,144	4,420	18,574	7,805	1,905	33,840	(23,501)
PEND OREILLE	1,089	13,068	6,580	7,831	2,570	795	18,000	(7,502)
PIERCE	5,668	68,016	33,670	157,504	67,355	15,930	169,920	(169,259)
SAN JUAN	817	9,804	3,550	2,000	350	960	17,520	(8,066)
SKAGIT	1,696	20,352	12,180	31,986	13,020	3,360	35,840	(28,508)
SKAMANIA	665	7,980	4,970	19,074	8,005	825	15,360	(15,385)
SNOHOMISH	6,194	74,328	24,500	95,913	40,531	13,650	145,600	(111,803)
SPOKANE	4,816	57,792	18,490	84,458	36,260	9,270	118,560	(97,028)
STEVENS	1,171	14,052	9,090	17,536	6,666	1,635	34,320	(26,934)
THURSTON	5,344	64,128	12,880	51,934	21,851	10,275	109,600	(67,323)
WAHKIAKUM	368	4,416	3,070	-2,288	-1,564	600	11,040	(5,060)
WALLA WALLA	526	6,312	7,090	16,536	6,566	2,700	37,280	(37,534)
WHATCOM	2,502	30,024	11,430	51,391	21,945	5,910	69,520	(61,441)
WHITMAN	2,061	24,732	4,430	26,986	11,770	1,800	36,960	(23,998)
YAKIMA	3,853	46,236	12,780	72,296	31,320	6,945	89,200	(74,284)
Unknown	-	-	1,460	8,912	3,865	210	4,800	(8,665)
TOTAL	$ 82,729	$ 992,748	$ 418,455	$ 1,399,419	$ 580,353	$ 178,335	$ 2,200,400	(1,788,005)

Current or future costs do not include DOL or DOH, but include agency locations without current network service.

ECG MANAGEMENT CONSULTANTS

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

CONNECTION TYPES AND COST ESTIMATES

Connection Type	Connection Description	Purchase Cost	Install Cost	Maintenance Cost
56	56 kbs frame relay line connection between locations within a county and connected via hub within the cloud.	$4,331.00	$480.00	$1,920.00
CWAN	County WAN connection already established at this location.	$0.00	$0.00	$0.00
DOH	Already connected via the Department of Health INPHO wide area network.	$0.00	$0.00	$0.00
DOL	Already connected via the Department of Licensing wide area network.	$0.00	$0.00	$0.00
FB	Fiber connection between building locations within a city in a county.	$1,000.00	$1,100.00	$250.00
FL	Fiber connection to a router in a building already installed at a facility.	$250.00	$500.00	$25.00
LL56	Leased line 56 kbs connection within a city.	$4,331.00	$480.00	$1,920.00
LLT1	Leased line T1 kbs connection within a city.	$4,817.00	$575.00	$2,005.00
ML	Removal of existing DOL connection within a hub building (i.e., courthouse).	($4,288.00)	($480.00)	$1,914.00)
NC	No cost for replacing a second or third line at a given location for an agency.	$0.00	$0.00	$0.00
T1	Frame relay line connection from City B to City A (hub) inside the cloud.	$4,817.00	$575.00	$2,005.00

The "Workstation Number" is the estimate of the number of end user workstations that would be connected to the JIN for a particular agency at a given facility. The "WAN Utilization Factor" is a multiplier between 0.25 and 1.0 assigned to the type of agency based upon assumptions about the type of use the network would receive. The $60 is the estimate for one-time line installation costs for a particular agency location. APPENDIX C presents a listing of the WAN Utilization Factors assigned to the agency types.

*Operating Costs = Sum (((Workstation Number) * (WAN Utilization Factor)) * $640) * (City In or Out Cloud Multiplier) + $480 * (County DTS Flag)*

The "City In or Out Cloud Multiplier" is a multiplier of either 1 or 1.5 assigned to each city within the state to account for the increased cost of telecommunications service outside of established frame relay service areas. The County DTS Flag is a multiplier between 0 and 1.0 in 0.25 increments assigned to each county within the state, based upon distance to Olympia, to account for the costs of DIS Digital Transport Services. The $640 per year is the cost estimate for providing multiprotocol network connection services per workstation based upon the yearly costs of a 56K digital line shared between five users. The algorithm is linear, and the cost of growing the network to accommodate only one user per 56K bandwidth size is five times the currently calculated cost. APPENDIX D presents a listing of the counties and cities and identifies both the County DTS Flag and the City In or Out Multiplier ("Cloud Flag").

B. MINIMUM SHARING ALTERNATIVE

EXHIBIT XV, which follows this page, presents a schematic outlining the minimum sharing network alternative. This alternative is not based upon the fundamental design concept of network connectivity based upon a common state government POP within each county. Instead local agencies requiring access to state applications connect directly to the telecommunications service provider's network and maintain their own local infrastructures (LANs).

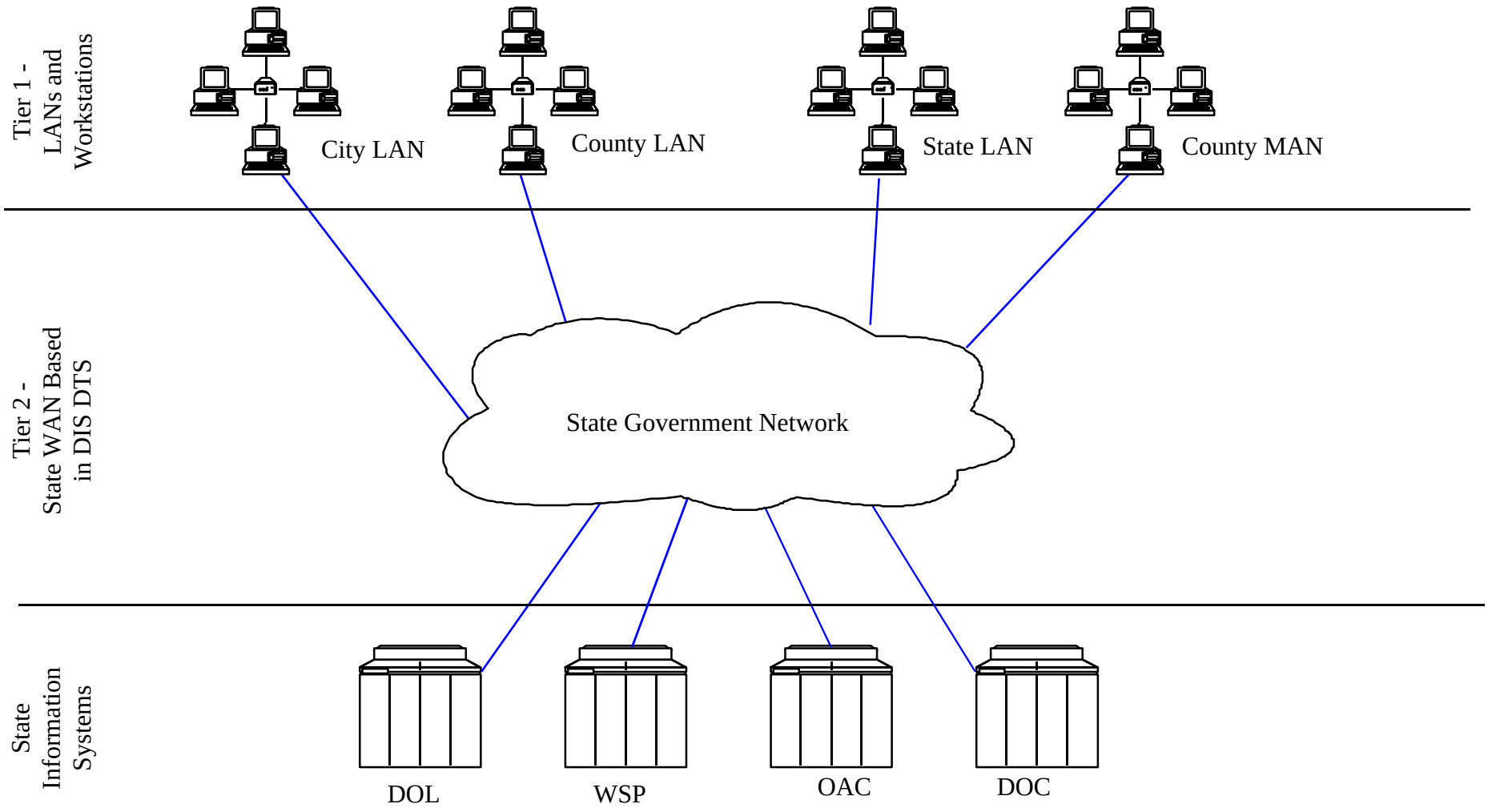
1. Strengths

JIN implementation under this alternative model has a number of positive impacts for development, implementation, and operation of the network. This alternative will:

- Meet requirements. The existing network infrastructures do not meet users' requirements or accessing multiple data sources and exchanging new data types. The new multiprotocol network will provide for increased access and data sharing.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

MINIMUM SHARING MODEL



- Centralize management. Elimination of the county infrastructures centralizes management of the network with the supporting organization.
- Increase agency control. All the network resources are in the control of the supporting agency to the extent that they control or contract for their support.

2. Weaknesses

There are several negative factors in considering the shared model for JIN. These include:

- Increased costs. Sharing of the network infrastructure between county and state networks minimizes the costs associated with multiple pieces of new equipment required to operate the multiprotocol network.
- Reduced data access. By not integrating into the county WAN infrastructures, this alternative can limit access to both state and local information.
- Fault tolerance. Reliance on one connection point to the WAN service provider creates a single point of failure and may decrease the overall reliability or fault tolerance of the system.

3. Costs

EXHIBIT XVI, which follows this page, presents the costs associated with implementing the JIN under the minimum sharing alternative for each agency. These estimates include the capital costs of equipment purchase and installation, as well as any line installation costs. Operating costs are calculated by the equipment maintenance costs and the line lease costs. The "No Agency" line in the exhibit is for those criminal justice agencies that were included in the database but currently have no network support by any of the other agencies. These are mostly small police departments, municipal courts, and county attorney offices. Equipment costs have been calculated as before by defining the type of WAN connection required to connect each criminal justice agency location to the JIN.

Line costs under this alternative are based upon the number of agency locations. Line lease installation costs were derived from the following formula for calculating the costs per criminal justice agency connection and from the data maintained in the agency location inventory.

*Installation Costs = Sum ($100 + ($100 * (City In or Out Cloud Multiplier))*
*+ $50 * (County DTS Flag))*

The "City In or Out Cloud Multiplier" and "County DTS Flag" fields are defined as above. The first $100 is the estimate for one-time line installation costs for a particular agency location. The second

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

MINIMUM SHARING ALTERNATIVE COST SUMMARY - BY AGENCY

Agency	Current Month	Current Year Cost	Equipment Install	Equipment Purchase	Equipment Maint./Yr.	Line Install	Line Maint./Yr.	Net Operating/Yr.
DOC	$ 15,849	$ 190,188	$ 38,015	$ 342,635	$ 151,765	$ 21,225	$ 246,300	$ (207,877)
DOL	-	-	-	-	-	-	-	-
OAC	32,996	395,952	54,240	489,403	216,960	27,063	318,900	(139,908)
WSP	33,884	406,608	113,565	1,023,574	453,375	86,663	994,800	(1,041,567)
No Agency	-	-	158,880	1,433,561	635,520	88,575	1,050,900	(1,686,420)
TOTAL	$ 82,729	$ 992,748	$ 364,700	$ 3,289,173	$ 1,457,620	$ 223,525	$ 2,610,900	$ (3,075,772)

$100 is the additional installation costs if the circuit is outside the frame relay cloud service area. The $50 is the estimate of DTS installation costs for those circuits that require this service.

*Operating Costs = Sum (12 * ($175 + ($100 * (City In or Out Cloud Multiplier - 1)))*
*+ $100 * (County DTS Flag))*

The $175 per month is the baseline cost estimate for providing multiprotocol network connection services per agency location based upon the yearly costs of a 56K digital line. The first $100 per month is the estimate of the additional costs if the agency is located outside the normal frame relay service cloud. The second $100 per month is the estimated cost of DTS services for those agency locations that will require it. All of the above costs have then been annualized. The algorithm is linear, and the cost of growing the network to accommodate only one user per 56K bandwidth size is five times the currently calculated cost.

C. RECOMMENDATIONS

The summary cost analysis table below has been derived from the previous alternative costs presented above. This table demonstrates that there is a variation of just over $1 million in capital costs and just under $1 million in yearly operating costs.

Network Alternative	Capital Costs		Operating Costs/Year	
	Equipment Purchase	Line Install	Equipment Maintenance	Line Leases
Current Network	$ 0	$ 0	--[3]	$ 992,748
Maximum Sharing	$1,154,184	$143,760	$390,128	$1,707,040
Minimum Sharing	$2,061,432	$134,950	$822,100	$2,238,600

While the costs of the two alternatives can be calculated, the actual implementation strategies must be based on the readiness, reliability, and support within the local jurisdictions. Some counties have developed and installed reliable WAN infrastructures that could be expanded to include all of the agency locations and have hired and trained knowledgeable support staff. Other counties do not have the infrastructure and/or the necessary staff.

It is therefore recommended that implementation of the JIN be based upon the readiness of the counties to support the shared alternative. JIN should be implemented under the shared alternative in

[3] Current network Equipment Maintenance for the DOL is included in the Line Leases costs. Line Leases costs are based upon the number of personnel requiring network access.

those counties that have developed and installed the technical and managerial support necessary to operate a network of this magnitude in this business environment. This includes the implementation of the security provisions required to ensure data quality and limit access to authorized users.

JIN can be implemented under the minimum sharing alternative in those counties that do not have required infrastructure in place. The sharing of network resources then would be left up to any agreements that may be created between organizations.

X. CONFORMITY WITH AGENCY STRATEGIC PLANS

X. CONFORMITY WITH AGENCY STRATEGIC PLANS

Each of the three primary agencies involved in this project (WSP, OAC, and DOC) has already begun implementation of a WAN for its users or customers. This is in support of the agency strategic plans and information technology plans.

XI. PROJECT MANAGEMENT AND ORGANIZATION

XI. PROJECT MANAGEMENT AND ORGANIZATION

The oversight and management structure for the JIN implementation would be based upon the criminal justice information technology governance structure already in place. This structure, which includes OFM management and system user representatives, is presented in EXHIBIT XVII, which follows this page. Presented below are descriptions of the entities identified in this structure and their respective roles and responsibilities related to the implementation of JIN.

A. INFORMATION SERVICES BOARD

The ISB provides policy direction and oversight on all information technology-related projects approved and funded by the state. This includes providing direction on statewide telecommunications policy. The ISB's role in JIN is to ensure that the criminal justice telecommunications needs and network implementation is consistent with the overall state infrastructure.

B. JUSTICE INFORMATION COMMITTEE

The JIC is a subcommittee of the state ISB and is responsible for providing executive oversight and making policy decisions. This committee would provide oversight on this project. The directors of the agencies included in this project are members of the JIC, as well as OFM, DIS, and representatives from all the local criminal justice functions. Responsibilities of the JIC are defined as follows:

- Approves and sponsors the JIN Implementation Plan once it is developed.
- Approves any funding allocations to JIN from federal and state grant funds.
- Reviews and responds to the activities and recommendations of the Executive Committee.
- Approves any changes to the project scope.

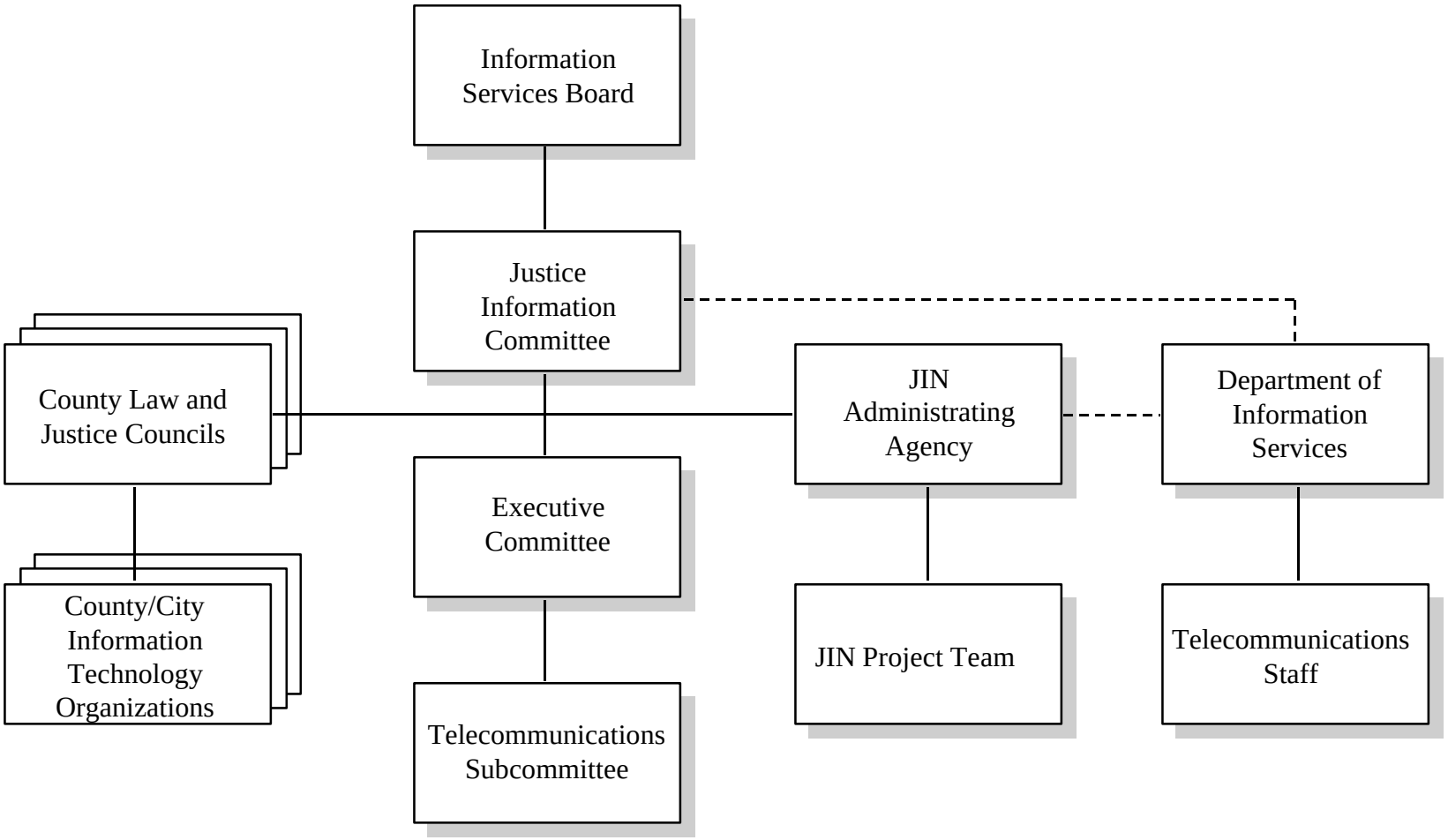
C. EXECUTIVE COMMITTEE

The project steering committee would be the Executive Committee for the Implementation of the Criminal Justice Information Act. This committee consists of key criminal justice stakeholders from state and local government throughout Washington's criminal justice community. Members include OAC, DOC, DIS, local law enforcement, superior court clerks, and prosecuting attorneys. The

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

EXHIBIT XVI

PROJECT GOVERNANCE STRUCTURE



ECG MANAGEMENT CONSULTANTS

committee oversees the project's progress and makes policy decisions that are beyond the scope of the project team. The responsibilities of the Executive Committee related to JIN are:

- Approving the overall project budget and modifications with review by the JIC.
- Evaluating and approving technical system designs to ensure compatibility prior to development and implementation.
- Reviewing progress on all projects relating to the JIN Implementation Plan.
- Recommending new projects and priorities to the JIC for its approval.
- Implementing the JIN Implementation Plan, which is defined in general terms by the JIC.
- Approving projects prior to sending the request to the legislature.
- Modifying the project schedule to ensure completion in a timely fashion. Any modifications that delay the final completion date must be approved by the JIC.
- Establishing voluntary and/or mandatory standards for all components of the JIN.

D. TELECOMMUNICATIONS SUBCOMMITTEE

In support of the Executive Committee, a number of subcommittees or task forces have been created to provide detailed direction of particular issues or projects. This includes a Telecommunications Subcommittee. The responsibilities of the Telecommunications Subcommittee are:

- Providing technical guidance on the development of project areas.
- Reviewing specific topical proposals and making technical recommendations for approval to the Executive Committee.

E. ADMINISTRATING AGENCY

In order to effectively administer the implementation of the JIN, one state agency must be assigned the responsibility of project management. This agency would be responsible for the administration of JIN implementation and the hiring and/or assigning of a project manager and staff. The Administrating Agency responsibilities for this project are defined as follows:

- Administers project funds and has the authority to make payments for the JIN Implementation Plan.
- Hires and manages the staff resources required to plan, manage, and coordinate the project among state agencies and local jurisdictions.
- Authorized to make project payments when all of the following three conditions are met:
  - » The expenditure is approved by the Executive Committee and any and all oversight milestones have been met.
  - » The expenditure is part of the JIN Implementation Plan, as defined by the JIC.
  - » The expenditure is no more than $250,000.
- Coordinates project implementation with JIN Project Manager and the Executive Committee.

F. JIN PROJECT TEAM

The JIN Project Team will work for the Administrating Agency. The project team will comprise a project manager and support staff to work with the Administrating Agency and DIS in implementation of the network. This is similar to the management structure used by the Department of Health with the INPHO project. Project management will be provided by an agency manager working closely with DIS, which is providing much of the installation and operation service. The project manager will have to be assigned to a particular agency, with reporting relationships to each of the state agencies involved. The responsibilities of the JIN project manager are:

- Developing and maintaining the JIN Implementation Plan.
  - » Maintaining the project schedule and budget.
  - » Managing project communications.
- Reporting JIN Implementation Plan and project progress to interested parties (agencies, associations, legislature, etc.).
- Reviewing and reporting on planning, management, and implementation of the tactical projects included in the JIN Implementation Plan.
- Providing quarterly project status reports to the JIC.
- Providing monthly project status reports to the Executive Committee.

G. COUNTY LAW AND JUSTICE COUNCILS

The County Law and Justice Councils have identified information technology and data sharing as a primary goal for improving criminal justice services. Since the implementation of JIN will require physical network integration within the confines of a county, these councils must take a major role in overseeing implementation of the networks within their jurisdictions. Most of the councils have broad representation of agency heads from all of the city and county criminal justice agencies. The responsibilities of the County Law and Justice Councils for JIN are:

- Developing and reviewing network implementation plans for its county.
- Providing policy and management direction to the county and city agencies involved in JIN.
- Coordinating the implementation of the network improvements among affected agencies.

H. DEPARTMENT OF INFORMATION SERVICES

The DIS provides telecommunications services to state and local agencies. As part of JIN, DIS will be responsible for the actual technical implementation and management of network infrastructure. DIS telecommunications staff will work with the JIN Project Manager and the Administrating Agency to ensure proper planning and management of the implementation of the network resources at state and local levels.

XII. INCREMENTAL COSTS

XII. INCREMENTAL COSTS

This section presents the costs associated with implementation of this new network infrastructure. EXHIBIT XVIII, which follows this page, presents network development and operational costs using the four DIS cost forms. EXHIBIT XIX - Equipment Cost Summary, which follows EXHIBIT XVIII, breaks down the costs associated with hardware, software, and network management services identified in the previous section as equipment costs. This information was calculated directly from the agency location inventory. The cost calculations used in these forms are described below.

A. ASSUMPTIONS AND CLARIFICATIONS

In order to put the estimated development and operating costs into the proper perspective, the following assumptions and clarifications have been identified:

- The infrastructure-related applications identified in Section VII.C, Application Model, are not included in the JIN network cost calculations. These applications include the messaging and electronic transfer applications that are required to exchange information between computer systems.
- The cost of the modifications to the primary or strategic business applications (DISCIS, WASIS, OBTS, etc.) are not included in the cost estimates. These application modifications would be required in order to increase user access and electronically exchange information.

These key components of a revised criminal justice information technology infrastructure are required in order to take full advantage of the potential benefits associated with the JIN. While the costs of these components are not included in the network feasibility study, some of the enhancements of the business applications and implementation of the infrastructure are already being planned to be completed during the network implementation time frame.

B. DEVELOPMENT COSTS

EXHIBIT XVIII, Form 2, presents the incremental costs associated with development of the new network. These costs sum to $3,797,444 and have been derived from the costs associated with the agency location inventory and security, plus costs for project management, security administration, and travel. Object Codes A and B are the salary and benefits costs for a project manager and three supporting staff members. Object Code E represents the equipment and network line costs associated

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

SUMMARY COST-BENEFIT AND CASH FLOW ANALYSIS

Form 1

	FY 1998	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	Grand Total
TOTAL OUTFLOWS	$1,235,271	$1,618,116	$2,137,524	$2,793,496	$3,586,031	$3,167,950	$3,167,950	$3,167,950	$3,167,950	$3,167,950	$27,210,188
TOTAL INFLOWS	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
NET CASH FLOW	($1,235,271)	($1,618,116)	($2,137,524)	($2,793,496)	($3,586,031)	($3,167,950)	($3,167,950)	($3,167,950)	($3,167,950)	($3,167,950)	
INCREMENTAL NPV		($2,644,127)	($4,490,601)	($6,788,817)	($9,598,566)	($11,962,539)	($14,213,942)	($16,358,136)	($18,400,224)	($20,345,071)	
CUMULATIVE COSTS		$2,853,387	$4,990,911	$7,784,407	$11,370,438	$14,538,388	$17,706,338	$20,874,288	$24,042,238	$27,210,188	
CUMULATIVE BENEFITS		$0	$0	$0	$0	$0	$0	$0	$0	$0	

Cost of Capital	Break-Even Period -Years[1] Non-discounted	Discounted	NPV $	IRR %
5.00%	+10	+10	($20,345,071)	#DIV/0!

[1] "Nondiscounted" represents break-even period for cumulative costs and benefits (no consideration of the time value of money).
"Discounted" considers the effect of the time value of money through incremental Net Present Value.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COST CASH FLOW ANALYSIS

Form 2

DEVELOPMENT PHASE[1]												
Incremental Costs	**OFM Object Codes**	**FY 1998**	**FY 1999**	**FY 2000**	**FY 2001**	**FY 2002**	**FY 2003**	**FY 2004**	**FY 2005**	**FY 2006**	**FY 2007**	**Grand Total**
Salaries and Wages	(A)	$170,000	$170,000	$170,000	$170,000	$170,000						$850,000
Employee Benefits	(B)	59,500	59,500	59,500	59,500	59,500						297,500
Personal Service Contracts	(CA)											0
Communications	(EB)											0
Hardware Rent/Lease	(ED)											0
Hardware Maintenance	(EE)											0
Software Rent/Lease	(ED)											0
Software Maintenance and Upgrade	(EE)											0
DIS Goods/Services	(EL)											0
Goods/Services Not Listed	(E)	76,413	76,413	76,413	76,413	76,413						382,065
Travel	(G)	15,000	15,000	15,000	15,000	15,000						75,000
Hardware Purchase Capitalized	(JC)	284,360	284,360	284,360	284,360	284,360						1,421,799
Software Purchase Capitalized	(JC)	154,216	154,216	154,216	154,216	154,216						771,080
Hardware Purchase - Noncapitalized	(KA)											0
Software Purchase - Noncapitalized	(KA)											0
Hardware Lease/Purchase	(P)											0
Software Lease/Purchase	(P)											0
Other (Specify)	( )											0
TOTAL DEVELOPMENT		$759,489	$759,489	$759,489	$759,489	$759,489	$0	$0	$0	$0	$0	$3,797,444

OPERATIONS PHASE[2] (Per Form 3 - Column C)												
Salaries and Wages	(A)	$170,000	$170,000	$170,000	$170,000	$170,000	$170,000	$170,000	$170,000	$170,000	$170,000	$1,700,000
Employee Benefits	(B)	59,500	59,500	59,500	59,500	59,500	59,500	59,500	59,500	59,500	59,500	595,000
Personal Service Contracts	(CA)	0	0	0	0	0	0	0	0	0	0	0
Communications	(EB)	0	0	0	0	0	0	0	0	0	0	0
Hardware Rent/Lease	(ED)	0	0	0	0	0	0	0	0	0	0	0
Hardware Maintenance	(EE)	38,787	77,574	116,361	155,148	193,935	193,935	193,935	193,935	193,935	193,935	1,551,480
Software Rent/Lease	(ED)	0	0	0	0	0	0	0	0	0	0	0
Software Maintenance and Upgrade	(EE)	18,317	36,633	54,950	73,266	91,583	91,583	91,583	91,583	91,583	91,583	732,664
DIS Goods/Services	(EL)	308,538	753,638	1,335,302	2,053,530	2,908,320	3,249,728	3,249,728	3,249,728	3,249,728	3,249,728	23,607,968
Goods/Services Not Listed	(E)	(119,359)	(238,718)	(358,078)	(477,437)	(596,796)	(596,796)	(596,796)	(596,796)	(596,796)	(596,796)	(4,774,368)
Travel	(G)	0	0	0	0	0	0	0	0	0	0	0
Hardware Purchase Capitalized	(JC)	0	0	0	0	0	0	0	0	0	0	0
Software Purchase Capitalized	(JC)	0	0	0	0	0	0	0	0	0	0	0
Hardware Purchase - Noncapitalized	(KA)	0	0	0	0	0	0	0	0	0	0	0
Software Purchase - Noncapitalized	(KA)	0	0	0	0	0	0	0	0	0	0	0
Hardware Lease/Purchase	(P)	0	0	0	0	0	0	0	0	0	0	0
Software Lease/Purchase	(P)	0	0	0	0	0	0	0	0	0	0	0
Other (Specify)	( )	0	0	0	0	0	0	0	0	0	0	0
TOTAL OPERATIONS		$475,782	$858,627	$1,378,036	$2,034,007	$2,826,542	$3,167,950	$3,167,950	$3,167,950	$3,167,950	$3,167,950	$23,412,744

TOTAL OUTFLOWS		$1,235,271	$1,618,116	$2,137,524	$2,793,496	$3,586,031	$3,167,950	$3,167,950	$3,167,950	$3,167,950	$3,167,950	$27,210,188
CUMULATIVE COSTS			$2,853,387	$4,990,911	$7,784,407	$11,370,438	$14,538,388	$17,706,338	$20,874,288	$24,042,238	$27,210,188	

[1] Reflects the applicable number of years for project development.

[2] Reflects the applicable number of years for project operations (must reflect at least 5 years after implementation or until payback for the system is achieved).

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
COSTS OF CURRENT METHOD VERSUS COSTS OF PROPOSED METHOD

Form 3

Operations Costs	Obj. Codes	FY 1998 (a) Current	FY 1998 (b) Project	FY 1998 (to Form 2)	FY 1999 (a) Current	FY 1999 (b) Project	FY 1999 (to Form 2)	FY 2000 (a) Current	FY 2000 (b) Project	FY 2000 (to Form 2)	FY 2001 (a) Current	FY 2001 (b) Project	FY 2001 (to Form 2)	FY 2002 (a) Current	FY 2002 (b) Project	FY 2002 (to Form 2)
Salaries and Wages	(A)		$170,000	$170,000		$170,000	$170,000		$170,000	$170,000		$170,000	$170,000		$170,000	$170,000
Employee Benefits	(B)		$59,500	59,500		$59,500	59,500		$59,500	59,500		$59,500	59,500		$59,500	59,500
Personal Service Contracts	(CA)			0			0			0			0			0
Communications	(EB)			0			0			0			0			0
Hardware Rent/Lease	(ED)			0			0			0			0			0
Hardware Maintenance	(EE)		$38,787	38,787		$77,574	77,574		$116,361	116,361		$155,148	155,148		$193,935	193,935
Software Rent/Lease	(ED)			0			0			0			0			0
Software Maintenance and Upgrade	(EE)		18,317	18,317		36,633	36,633		54,950	54,950		73,266	73,266		91,583	91,583
DIS Goods/Services	(EL)	$395,952	704,490	308,538	$395,952	1,149,590	753,638	$395,952	1,731,254	1,335,302	$395,952	2,449,482	2,053,530	$395,952	3,304,272	2,908,320
Goods/Services Not Listed	(E)	596,796	477,437	(119,359)	596,796	358,078	(238,718)	596,796	238,718	(358,078)	596,796	119,359	(477,437)	596,796	0	(596,796)
Travel	(G)			0			0			0			0			0
Hardware Purchase Capitalized	(JC)			0			0			0			0			0
Software Purchase Capitalized	(JC)			0			0			0			0			0
Hardware Purchase - Noncapitalized	(KA)			0			0			0			0			0
Software Purchase - Noncapitalized	(KA)			0			0			0			0			0
Hardware Lease/Purchase	(P)			0			0			0			0			0
Software Lease/Purchase	(P)			0			0			0			0			0
Other (Specify)	( )			0			0			0			0			0
TOTAL OPERATION COSTS		$992,748	$1,468,530	$475,782	$992,748	$1,851,375	$858,627	$992,748	$2,370,784	$1,378,036	$992,748	$3,026,755	$2,034,007	$992,748	$3,819,290	$2,826,542
FTEs			4	4		4	4		4	4		4	4		4	4

Operations Costs	Obj. Codes	FY 2003 (a) Current	FY 2003 (b) Project	FY 2003 (to Form 2)	FY 2004 (a) Current	FY 2004 (b) Project	FY 2004 (to Form 2)	FY 2005 (a) Current	FY 2005 (b) Project	FY 2005 (to Form 2)	FY 2006 (a) Current	FY 2006 (b) Project	FY 2006 (to Form 2)	FY 2007 (a) Current	FY 2007 (b) Project	FY 2007 (to Form 2)
Salaries and Wages	(A)		$170,000	$170,000		$170,000	$170,000		$170,000	$170,000		$170,000	$170,000		$170,000	$170,000
Employee Benefits	(B)		$59,500	59,500		$59,500	59,500		$59,500	59,500		$59,500	59,500		$59,500	59,500
Personal Service Contracts	(CA)			0			0			0			0			0
Communications	(EB)			0			0			0			0			0
Hardware Rent/Lease	(ED)			0			0			0			0			0
Hardware Maintenance	(EE)		$193,935	193,935		$193,935	193,935		$193,935	193,935		$193,935	193,935		$193,935	193,935
Software Rent/Lease	(ED)			0			0			0			0			0
Software Maintenance and Upgrade	(EE)		91,583	91,583		91,583	91,583		91,583	91,583		91,583	91,583		91,583	91,583
DIS Goods/Services	(EL)	$395,952	3,645,680	3,249,728	$395,952	3,645,680	3,249,728	$395,952	3,645,680	3,249,728	$395,952	3,645,680	3,249,728	$395,952	3,645,680	3,249,728
Goods/Services Not Listed	(E)	596,796	0	(596,796)	596,796	0	(596,796)	596,796	0	(596,796)	596,796	0	(596,796)	596,796	0	(596,796)
Travel	(G)			0			0			0			0			0
Hardware Purchase Capitalized	(JC)			0			0			0			0			0
Software Purchase Capitalized	(JC)			0			0			0			0			0
Hardware Purchase - Noncapitalized	(KA)			0			0			0			0			0
Software Purchase - Noncapitalized	(KA)			0			0			0			0			0
Hardware Lease/Purchase	(P)			0			0			0			0			0
Software Lease/Purchase	(P)			0			0			0			0			0
Other (Specify)	( )			0			0			0			0			0
TOTAL OPERATION COSTS		$992,748	$4,160,698	$3,167,950	$992,748	$4,160,698	$3,167,950	$992,748	$4,160,698	$3,167,950	$992,748	$4,160,698	$3,167,950	$992,748	$4,160,698	$3,167,950
FTEs			4	4		4	4		4	4		4	4		4	4

Network implementation phased in over 5 years.
Network user bandwidth requirements increased 5 fold over 5 years and then flattens out.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

BENEFITS CASH FLOW ANALYSIS

Form 4

Tangible Benefits	OFM Object Codes	BENEFITS FY 1998	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	Grand Total
Hard $												
Revenues (Specify)	(revenue codes)											
												$0
												$0
												$0
												$0
												$0
Reimbursements (Specify)	(object codes)											
												$0
												$0
												$0
												$0
												$0
Cost Reduction (Specify) [1]	(object codes)											
												$0
												$0
												$0
												$0
												$0
Other (Specify) [2]	(object codes)											
												$0
												$0
												$0
												$0
												$0
Soft $												$0
Cost Avoidance (Specify)	(object codes)											
												$0
												$0
												$0
												$0
												$0
Other (Specify)	(object codes)											
												$0
												$0
												$0
												$0
												$0
TOTAL INFLOWS		$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0
CUMULATIVE BENEFITS			$0	$0	$0	$0	$0	$0	$0	$0	$0	

[1] Reflects all Cost Reduction Benefits except Operations reductions (which are reflected in Cost of Operations).

[2] Includes public benefits under "Other."

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
EQUIPMENT COST SUMMARY

EXHIBIT XIX

Network Equipment Unit Description	Unit Purchase Cost	Unit Installation Cost	Unit Maintenance Cost	Number of Units	Total Purchase Cost	Total Installation Cost	Total Maintenance Cost
Hardware							
Cisco 2501 Router	$968	$189	$170	186	$180,048	$35,154	$31,620
Cisco 2514 Router	$1,454	$284	$255	7	$10,178	$1,988	$1,785
DTE V.35 Cable	$105	$0	$0	193	$20,265	$0	$0
Kentrox Datasmart (DSU/CSU)	$1,400	$271	$290	193	$270,200	$52,303	$55,970
Kentrox V35-DB25 Interface	$23	$0	$0	193	$4,439	$0	$0
Kentrox RJ48c Plug	$98	$0	$0	193	$18,914	$0	$0
508B Transceiver Cable	$134	$20	$23	193	$25,862	$3,860	$4,439
903-A AUI Cable	$43	$0	$6	201	$8,643	$0	$1,206
Fiber Extension	$250	$500	$25	143	$35,750	$71,500	$3,575
Fiber Optical Transceiver	$250	$50	$25	70	$17,500	$3,500	$1,750
Fiber Extension to Building	$500	$1,000	$200	70	$35,000	$70,000	$14,000
Subtotal Hardware:					$626,799	$238,305	$114,345
Software							
IP/IPX Software	$1,560	$0	$0	193	$301,080	$0	$0
Software Upgrades - Flash	$0	$0	$231	193	$0	$0	$44,583
Subtotal Service:					$301,080	$0	$44,583
Service							
Network Management	$0	$0	$1,200	193	$0	$0	$231,600
Subtotal Service:					$0	$0	$231,600
			Total Costs:		$927,879	$238,305	$390,528

ECG MANAGEMENT CONSULTANTS

with installation split over 5 years. Object Code JC costs are for purchase of the hardware and software required based upon the agency location connection type calculations generated from the model.

C. OPERATIONAL COSTS

Operation of the new network increases the yearly costs for the three agencies (DOC, WSP, and OAC) from $992,748 to $4,160,698, an increase of $3,167,950 per year. These costs are divided between hardware maintenance, software maintenance and upgrades, and leased network line costs. Also included in these costs are the estimates for network security software maintenance and administrative personnel. The operational costs assume a 20 percent network replacement each year of the 5-year project and a 20 percent increase in demand for network bandwidth each year for fiscal year (FY) 1999 through FY 2003. It is assumed that network bandwidth requirements remain stable after that phase of increase. These potential operating cost estimates do not factor in any decrease in costs that may result from advances in technology.

XIII. BENEFITS

XIII. BENEFITS

This section of the feasibility study presents the tangible and intangible benefits associated with the implementation of the JIN.

A. TANGIBLE BENEFITS

Development and implementation of the new multiprotocol network will provide the infrastructure necessary to develop capabilities to exchange information electronically between all of the connected criminal justice organizations. The Cost-Benefit Model included with this feasibility study was developed to assist in quantifying the potential cost savings associated with the implementation of electronic data exchange capabilities. This model demonstrates that the criminal justice community may be able to save considerably in terms of the clerical and administrative costs associated with manually exchanging information.

B. INTANGIBLE BENEFITS

The majority of the benefits associated with JIN implementation are not quantifiable and are therefore defined as intangible. Intangible benefits resulting from implementing JIN are detailed below.

- Meets Requirements. The current network infrastructure does not meet the needs of crime information users and is structured such that implementation of new capabilities is not feasible. This is due to the fact that the current networks were designed only for data transfer, not multimedia capabilities. Network migration would allow the state to satisfy known current and upcoming requirements (e.g., NCIC 2000).
- Enhanced capabilities. The migration of JIN would significantly enhance local criminal justice agencies by providing new capabilities. Agencies and users would be able to communicate information electronically via e-mail using multiple information types.
- Increased expandability. Implementation of the network under a shared model provides increased access to those agencies already connected to a network. It also allows additional agencies to access criminal justice information.
- Increased system flexibility, adaptability, and expandability. The new network provides for greater expandability by allowing new users to be quickly added on by local jurisdictions.

- Better access. The new network provides access to multiple state and local applications and information from the same workstations.
- Increased intercounty information exchange. The new network establishes the capability for direct intercounty information exchange.
- Enhanced development environment. The new network provides an environment for developing new applications based on Internet technology.
- Better positioning for new technology. The new network positions the agencies to utilize emerging network technology and potential integration of voice, data, images, and video.
- Increased officer safety. Field officers will be able to readily identify potential threats to their safety, as well as public safety, through increased access to information.
- Increased efficiency. Efficient use of resources will be increased through reduced duplicate entry of information.

Overall, JIN will greatly increase the effectiveness of law enforcement, courts, and correction operations around the state of Washington. The new network will provide criminal justice practitioners with broader access to key criminal justice information. In addition, facilities that improve access to criminal justice information enhance the speed, accuracy, safety, and effectiveness of criminal justice actions.

XIV. RISK MANAGEMENT

XIV. RISK MANAGEMENT

This section of the study presents an assessment that rates the potential level of risk (potential for project failure) of the JIN project. The purpose of this assessment is to identify areas of the project that may contain an unusually high level of risk and may require corrective action or greater levels of monitoring. In order to assess this risk, the project was evaluated against eight major project risk areas using the criteria presented in the Risk Assessment Model described in APPENDIX E.

EXHIBIT XX, which follows this page, presents the results of the baseline risk assessment. As presented on this exhibit the overall risk rating for the project has been identified at 54 percent. Although there is risk across all areas of the project, there are some risk criteria with a high rating of 3 or 4. These risk areas are discussed below and, where appropriate, a mitigation strategy has been identified:

1. Project Management

   1.2 Project Commitment (3) - Since this project covers more than one agency, no project manager has been assigned. **Mitigation**: A permanent project manager should be selected to work with DIS on the implementation.

   1.5 Project Management Relationships (3) - A project manager position currently does not exist and given that the project spans more than one agency, the manager relationships are critical to success. **Mitigation**: The person selected as project manager must be approved by all of the agencies involved.

2. Customer Involvement

   2.1 Customer Acceptance (3) - The agencies involved in the project implementation recommendation must work closely with the county organizations involved. This acceptance will be necessary to implement the network successfully. **Mitigation**: The project manager and lead agencies must communicate clearly with the local jurisdictions.

   2.2 Customer Responsibility (3) - Responsibility for this project has not been assigned to any particular agency. **Mitigation**: Assign project responsibility to one agency or to DIS.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

PROJECT RISK ASSESSMENT

	Category	Risk Rating	x	Wgt.	Risk Score	Risk %
1.0	Project Management					
1.1	Project Management Experience	1 **2** 3 4	x	5	10	
1.2	Project Commitment	1 2 **3** 4	x	5	15	
1.3	Project Manager Authority	1 **2** 3 4	x	5	10	
1.4	Project Management Approach	1 **2** 3 4	x	5	10	
1.5	Project Management Relationships	1 2 **3** 4	x	5	15	
	Project Management					60%
2.0	Customer Involvement					
2.1	Customer Acceptance	1 2 **3** 4	x	5	15	
2.2	Customer Responsibility	1 2 **3** 4	x	5	15	
2.3	Customers on Project Team	1 **2** 3 4	x	5	10	
2.4	Customer Experience	1 **2** 3 4	x	5	10	
2.5	Customer Justification	1 **2** 3 4	x	5	10	
	Customer Involvement					60%
3.0	Organization					
3.1	Agency Experience	1 2 **3** 4	x	5	15	
3.2	Executive Management Involvement	1 **2** 3 4	x	5	10	
3.3	Management Cohesiveness	1 **2** 3 4	x	5	10	
3.4	Organizational Stability	**1** 2 3 4	x	5	5	
3.5	External Funding	1 **2** 3 4	x	5	10	
	Organization					50%
4.0	Technology					
4.1	Hardware Experience	1 **2** 3 4	x	5	10	
4.2	Software Experience	1 **2** 3 4	x	5	10	
4.3	Methodology Experience	1 **2** 3 4	x	5	10	
4.4	Quality Assurance	**1** 2 3 4	x	5	5	
4.5	Project Staff Technical Training	1 **2** 3 4	x	5	10	
	Technology					45%
5.0	Scope					
5.1	Project Scope Size	**1** 2 3 4	x	5	5	
5.2	Change Control Management	1 **2** 3 4	x	5	10	
5.3	Requirements Diversity	**1** 2 3 4	x	5	5	
5.4	Work Plan	**1** 2 3 4	x	5	5	
5.5	Available Resources	1 **2** 3 4	x	5	10	
	Scope					35%
6.0	Oversight					
6.1	Monitoring Process	1 **2** 3 4	x	5	10	
6.2	DIS Involvement	**1** 2 3 4	x	5	5	
6.3	Procurement Process	1 **2** 3 4	x	5	10	
6.4	Milestone Reviews	1 **2** 3 4	x	5	10	
6.5	Status Reporting	1 **2** 3 4	x	5	10	
	Oversight					45%

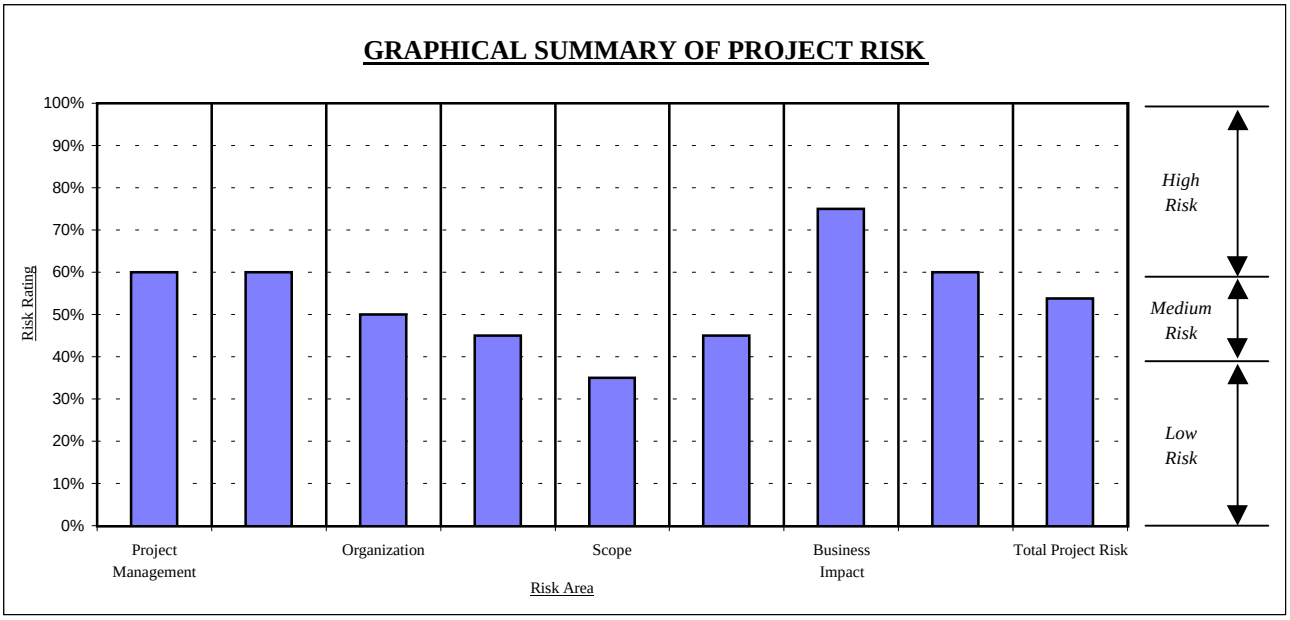
ECG MANAGEMENT CONSULTANTS

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

PROJECT RISK ASSESSMENT

	Category	Risk Rating	x	Wgt.	Risk Score	Risk %
7.0	Business Impact					
7.1	Agency Mission/Program Impact	1 2 3 **4**	x	5	20	
7.2	Customer Impact	1 2 **3** 4	x	5	15	
7.3	Change in Customer Service	1 **2** 3 4	x	5	10	
7.4	Technology Dependence	1 2 **3** 4	x	5	15	
7.5	Performance Requirements	1 2 **3** 4	x	5	15	
	Business Impact					75%
8.0	Cost-Benefit					
8.1	Budget Size	1 **2** 3 4	x	5	10	
8.2	Achievable Benefits	1 **2** 3 4	x	5	10	
8.3	Economic Justification	1 2 **3** 4	x	5	15	
8.4	Elapsed Time	1 2 **3** 4	x	5	15	
8.5	Cost Control	1 **2** 3 4	x	5	10	
	Cost-Benefit					60%
	TOTAL PROJECT RISK				430	54%

GRAPHICAL SUMMARY OF PROJECT RISK



ECG MANAGEMENT CONSULTANTS

3. Organization

3.1 Agency Experience (3) - The agencies involved (including DIS) do not have recent significant experience with implementation of these new networking technologies and of this magnitude. **Mitigation**: Agencies should work with DIS to contract for any shortcomings in technical expertise.

7. Business Impact

7.1 Agency Mission/Program Impact (4) - The new network is critical to the successful operation of each agency involved. **Mitigation**: A conservative approach to implementing the network has been recommended to lessen the impact of network migration on the agencies.

7.2 Customer Impact (3) - All users of applications operating across this network will be affected by its implementation. **Mitigation**: Careful planning and testing will lessen the impact on the users, and their general acceptance will be important.

7.4 Technology Dependence (3) - Successful implementation of the network depends upon a number of new technologies and configurations. **Mitigation**: A conservative approach to implementing new technologies should be selected, in addition to comprehensive testing.

7.5 Performance Requirements (3) - The network's ability to meet the business performance requirements is critical. **Mitigation**: Clear performance benchmarks should be established for each agency type. Implementation of the network and its performance should be closely monitored against these benchmarks to ensure customer satisfaction.

8. Cost-Benefit

8.3 Economic Justification (3) - The benefits associated with the network migration are not tangible and the project has a significant operational cost increase. **Mitigation**: The costs of the network components and services are steadily decreasing and as new applications are developed, they will show positive benefits.

8.4 Elapsed Time (3) - Migration to the new network will take a number of years to fully implement. **Mitigation**: Identify key milestones consistent with the project implementation strategies to ensure that migration objectives are being met.

This assessment reflects a level of risk that is moderate; subsequent evaluations should be made at the beginning of each quarter and compared to this baseline.

XV. IMPLEMENTATION PLAN

XV. IMPLEMENTATION PLAN

This section presents the network implementation strategies, high-level task plan, and schedule for the JIN network infrastructure project.

A. OVERVIEW

The JIN implementation is broken down into four phases that will result in deployment of the network and staged migration from existing networking technology to the new network. In Phase I, the Executive Committee will confirm the implementation strategies, select a project manager, develop an agency implementation schedule, and update the project budget. In Phase II, the project team will develop the detailed networking and security architecture to satisfy client requirements, determine the most appropriate hardware and software to use in building the network, and establish the process for managing and operating the network once it is installed. In Phase III, the project team will select, install, and evaluate potential hardware and software products that meet the detailed design requirements. Phase IV of the network deployment strategy is implementation of the shared networking infrastructure and migration of clients from existing networks to the JIN.

B. IMPLEMENTATION STRATEGIES

The implementation plan for the network is based upon chosen strategies. The strategies define the migration options chosen for the implementation. Implementation strategies that have been identified for the JIN network implementation are:

- A multiagency project team will be formed to manage overall design and installation of the JIN.
- A single project manager will be responsible for working with DIS and each of the three agencies.
- The network will be implemented on a county-by-county basis, rather than on a state agency basis.
- Implementation will be based upon the network readiness and design of each county. Counties that can meet the network performance, security, and support requirements will be implemented first.
- The migration of the ACCESS network will take into account the multidrop nature of the existing network.

C. TASK PLAN

The project phases and high-level tasks required to complete implementation and migration to the new network infrastructure are listed below.

PHASE I - PROJECT PLANNING

The initial phase is for updating the project management plan. This includes confirming the implementation strategies, defining the project management structure, reviewing local agencies' readiness, developing an agency implementation schedule, and updating the project budget. Tasks to be completed during this phase of the project are described below.

Task 1 - Confirm Implementation Strategies

The first task is to confirm the identified implementation strategies. These strategies form the basis by which the project will be structured and implemented. Activities to be completed during this task include:

- Review and update implementation strategies.
- Propose a cost allocation model for approval.
- Present updated implementation strategies and cost allocation model to Executive Committee.
- Present implementation strategies to agency management committees.
- Update strategies based upon executive reviews.
- Finalize project implementation strategies.

Task 2 - Define Project Management Structure

In parallel with confirmation of the implementation strategies, the project management structure must be defined. This includes defining the overall governance structure and the project management structure. Activities to be completed during this task include:

- Define project governance structure.
- Define project management organization structure.

- Select project manager.
- Define project communications and reporting.

Task 3 - Review County Readiness

The feasibility study provided a detailed inventory of agency, county, and location network readiness. Network migration is based upon a county-centric implementation model, and the project team will require a detailed understanding of the readiness of each county. Activities to be completed during this task include:

- Review feasibility study agency location inventory.
- Define network security and support readiness requirements.
- Survey county network administrator as to readiness for migration.

Task 4 - Develop County Implementation Schedule

The next task is to develop a schedule or plan for migrating the network county by county. This plan will be in priority order, with the most-ready county being implemented first. Activities to be completed during this task include:

- Interview counties regarding their requirements for migration.
- Rank counties by readiness.
- Define any network implementation assumptions.
- Develop an implementation schedule based upon assumptions and county rankings.

Task 5 - Update Project Budget

The last task in this phase involves updating the project budget based upon current cost information. Network equipment costs will change over time, and the most current configuration estimates should be used. Activities to be completed during this task include:

- Review feasibility study cost assumptions.
- Update costs assumptions based upon current technical equipment configurations.
- Update the overall project budget with new parameters.

PHASE II - DETAILED NETWORK DESIGN

Once the project planning phase has been completed, the network design phase will begin. This phase updates the existing network and security designs based upon more current information and new technologies. It also develops the management and operations agreements required between agencies, between agencies and DIS, and between DIS and the counties. Tasks to be completed during this phase of the project are described below:

Task 6 - Update Detailed Network Design

With a detailed understanding of the clients' needs and a projection of the capacity requirements of the JIN, the next step in the implementation process is to update the overall network design. Based on information about the current state network infrastructure, the project team will be able to develop a WAN architecture that is appropriate for the clients' needs. As part of this activity, the project team must determine the location of each network client for each state agency participating in the JIN. Once the location of the routers has been established, interconnecting facilities (frame relay, private lines, or other transport) can be designed to provide required network throughput. Activities to be completed during this task include:

- Review current state network architecture.
- Review county readiness and architecture survey results.
- Develop detailed county-by-county network designs.
- Develop detailed network backbone design.

At the completion of this task, the project team will have created a design document that identifies the location of all network routers and the performance characteristics of each router. The design document will also identify the facilities for interconnecting the routers and the bandwidth requirements of those facilities.

Task 7 - Update Network Security Design

In conjunction with the network design, a specific security design must be developed. This design must accommodate the security requirements with a detailed methodology. Activities to be completed during this task include:

- Review the existing security design.
- Update network security requirements.

- Identify and evaluate new network security technologies.
- Identify alternative network security implementation mechanisms.
- Update network security design with chosen alternative(s).

Task 8 - Define Network Operations Agreements

With completion of the network design, the project team will need to work with the agencies participating in the JIN and the DIS to update the existing DIS service agreement for operating and managing the network. In this task, the project team will define an overall network management architecture and the tools and procedures to be used to support the JIN. The project team will work with the DIS and the agencies participating in the JIN to establish the network management roles to be performed by DIS and those to be performed by individual agencies. Activities to be completed during this task include:

- Review current network services agreement.
- Identify new agreement requirements and language.
- Draft new management and operations agreements.
- Distribute new agreements among participating agencies and organizations.
- Update agreements based upon comments from the review process.
- Finalize operating agreements.

PHASE III - PRODUCT EVALUATION

Once the detailed designs are complete, a number of products may or may not meet the requirements. Tasks to be completed during this phase of the project are described below.

Task 9 - Conduct Product Selection and Testing

Following completion of the overall network design and the network management architecture, specific products that will satisfy the performance and management criteria of the network will need to be identified. At the completion of this task, a detailed list of the hardware and software that will be required to install the network will have been created.

Task 10 - Conduct Field Trials

The purpose of the field trial is to validate the viability of the technology architecture developed in Phase I. The first activity in conducting a field trial is to select a trial site that is representative of a typical network site. A set of measurable acceptance criteria should be established to validate the relative success of the field trial. At a minimum, acceptance criteria should address the following items:

- Performance.
- Reliability.
- Support structure.
- Functionality.

The next activity will be to develop a detailed installation and conversion plan to address the following areas:

- Installation of data center hardware and software.
- Establishment of the frame relay PVCs.
- Installation of router hardware and software at the test site.
- Test plan for certifying the network infrastructure.
- Plan for supporting the client through the field trial.
- Network acceptance test plan.

Once the plan has been completed, it should be executed and the results of the acceptance test should be compared to preestablished objectives. If testing conducted during the field trial does not meet the preestablished objectives, the overall network architecture should be reviewed and modified to bring actual network performance in line with expectations.

At the end of this task, the project team will have validated the overall network architecture and will possess an installation plan template that can be reused for subsequent site installation.

PHASE IV - NETWORK DEPLOYMENT AND MIGRATION

The last phase of the project involves actual deployment and migration to the new network. This includes purchasing and installing the equipment, deploying the equipment at the desired locations, and facilitating migration of the users and organizations. Migration will be conducted as a partnership

between the state and local agencies. Tasks to be completed during this phase of the project are detailed below.

Task 11 - Update County Implementation Schedule

Once the network design and operational products are defined, the project team must update the county implementation schedule based upon the new information. The updated schedule will be the basis for the actual migration and will coordinate the project's activities from this point. This task involves development of a detailed implementation schedule that will outline the activities required to deliver the JIN to each county and the estimated dates for delivery. This will address the following four major activities:

- Establish migration/conversion priorities based on the existing and future communications requirements of each participating agency.
- Define the data center activities that are required to support the client migration and establish target completion dates.
- Conduct site surveys at each JIN POP to determine the level of effort required to install the JIN at that location.
- Define the activities required to implement the network management architecture defined in Phase II.

The items listed above will be compiled into a single integrated implementation plan that can be used for tracking the overall progress of the project and establishing interdependencies between activities.

Task 12 - Deploy Network Infrastructure

This task involves execution of the plan developed in Task 11. Deploying the network infrastructure will entail scheduling and tracking of activities at county hubs and in the data center. This will include the following activities:

- Order host access hardware and software.
- Manage the installation and certification of data center components.
- Order router hardware and software.
- Manage installation and certification of the routers at county hubs.
- Order frame relay PVCs to interconnect network sites.
- Manage the connection of each county hub to the network.

- Order, install, and certify the network management system.

At the completion of this task, the underlying network infrastructure of the JIN will be installed and certified and will conform to the network and network management architectures defined in Phase I.

Task 13 - Facilitate Client Migration

The final activity associated with installation of the JIN is to assist end users in migrating to the network. The following three activities are required to facilitate migration:

- Develop processes for the ongoing migration of clients from existing networks to the JIN.
- Define a technical support structure to provide assistance to clients during the migration process.
- Perform ongoing capacity analysis of the network through migration to ensure that levels of service remain within limits.

At the completion of this task, the project team will have created a set of procedures and processes that will enable clients to migrate to the JIN and will provide a support structure to facilitate the migration and ensure that the network's overall performance meets predefined performance standards.

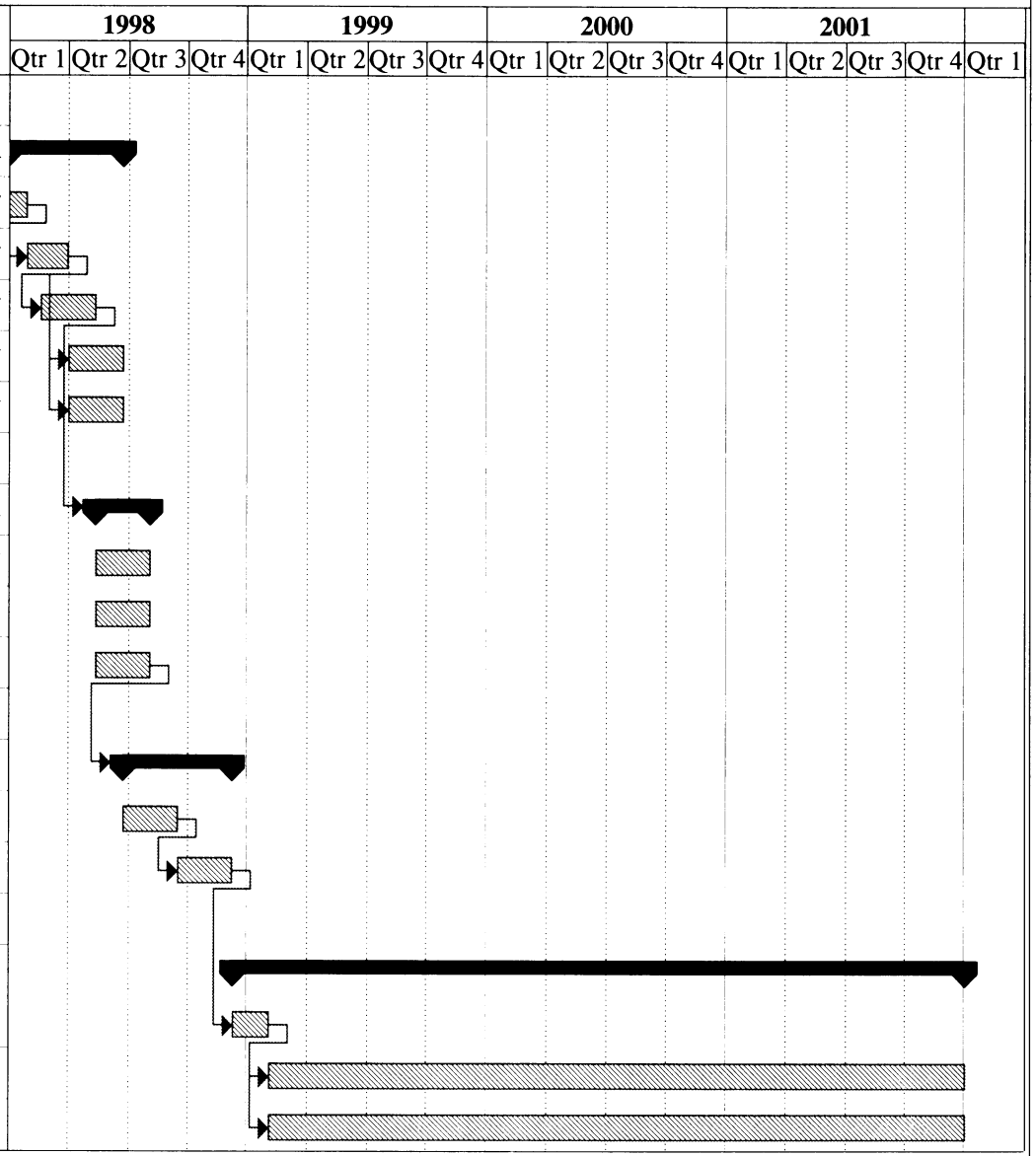
D. SCHEDULE

EXHIBIT XXI, which follows this page, presents the overall schedule for implementation of the network based upon the selected strategies and the task plan. Up to 5 years will be required to complete the migration.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
IMPLEMENTATION SCHEDULE

EXHIBIT XXI

WBS	Task Name	Duration
PHASE I	**PROJECT PLANNING**	**125d**
1	Confirm Implementation Strategies	4w
2	Define Project Management Structure	9w
3	Review County Readiness	12w
4	Develop County Implementation Schedule	12w
5	Update Project Budget	12w
PHASE II	**DETAILED NETWORK DESIGN**	**60d**
6	Update Detailed Network Design	12w
7	Update Detailed Security Design	12w
8	Define Network Operations Agreements	12w
PHASE III	**PRODUCT EVALUATION**	**120d**
9	Conduct Product Selection and Testing	12w
10	Conduct Field Trials	12w
PHASE IV	**NETWORK DEPLOYMENT**	**800d**
11	Update County Implementation Schedule	8w
12	Deploy Network Infrastructure	152w
13	Facilitate Client Migration	152w



F:\DOCSOPEN\37 | Task | Milestone | Summary | Progress

ECG MANAGEMENT CONSULTANTS

APPENDIX A
GLOSSARY

GLOSSARY

This glossary provides a reference for acronyms and terms used in the JIN Network Feasibility document. The primary source for this glossary is the Dictionary of Criminal Justice Data Terminology (Second Edition, 1981), published by the U.S. Department of Justice.

Term/Acronym	Definition
ACCESS	A Central Computerized Enforcement Service System. This is the messaging switch by which criminal justice agencies exchange information with WASIS and WACIC.
ATF	Bureau of Alcohol, Tobacco, and Firearms.
Arrest	Taking an adult or juvenile into physical custody by authority of law for the purpose of charging the person with a criminal offense or a delinquent act or status offense, terminating with the recording of a specific offense.
Batch Transaction	In this document, batch refers to the submission of transactions from another system in potentially large groups. These submissions may be made through system interfaces or manually (e.g., via tape).
Child and Adult Abuse Offense	A crime against a child under 16 years of age, a developmentally disabled person, or a vulnerable adult as defined in the Child and Adult Abuse Information Act. This includes civil adjudications and financial exploitation. See RCW 43.43.830 for additional details.
CAD	Computer-aided dispatch.
CJIS	Criminal justice information system.
Conviction	The judgment of a court, based on the verdict of a jury or judicial officer, or on the guilty plea or nolo contendere plea of the defendant, that the defendant is guilty of the offense(s) with which he or she has been charged. In Washington, a conviction refers to any finding that is adverse to the defendant.
Conviction Only Criminal History	Report that addresses only arrests that resulted in convictions and pending arrests that have been in process less than 1 year without disposition.

Term/Acronym	Definition
Court Order	A mandate, command, or direction issued by a judicial officer in the exercise of his/her judicial authority. Court orders include warrants, no-contact orders, restraining orders, protection orders, antiharassment orders, and special orders to avoid particular areas.
CRD	Criminal Records Division.
Crime	An act committed or omitted in violation of a law forbidding or commanding it for which the possible penalties for an adult upon conviction include incarceration, for which a corporation can be penalized by fine or forfeit, or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. Also referred to as criminal offense.
Criminal History	Information contained in records collected by criminal justice agencies on individuals, consisting of identifiable descriptions and notations of arrests, detentions, indictments, information or other formal criminal charges, and any disposition arising therefrom, including sentences, correctional supervision, and release. In Washington, WASIS is the central repository for criminal history information.
Criminal Justice	Any activity pertaining to crime prevention, control, or reduction or enforcement of the criminal law, including, but not limited to, police efforts to prevent, control, or reduce crime or to apprehend criminals; activities of courts having criminal jurisdiction and related agencies (including prosecutorial and defender services); activities of corrections, probation, or parole authorities; and programs related to the prevention, control, or reduction of juvenile delinquency or narcotic addiction.
Criminal Justice Agency	A court or government agency that administers criminal justice pursuant to a statute or executive order that allocates a substantial part of its budget to the administration of criminal justice.
CSD	Computer Services Division.
DBMS	Database Management System.
DIS	Washington State Department of Information Services.
DISCIS	District Court Information System.

Term/Acronym	Definition
DOC	Department of Corrections.
DOL	Department of Licensing.
FBI	Federal Bureau of Investigation.
Felony	A criminal offense punishable by incarceration of more than 1 year.
FORS	Felony Offender Reporting System. Maintained by DOC.
III	Interstate Identification Index. This index, maintained by the FBI, indicates individuals who have criminal history records in states that participate in the program.
JIN	Justice Information Network.
JUVIS	Juvenile Information System.
Law Enforcement Agency	A federal, state, or local criminal justice agency or identifiable subunit of which the principal functions are the prevention, detection, and investigation of crime and the apprehension of alleged offenders.
LEO	Law enforcement officer. An employee of a law enforcement agency who is sworn to carry out law enforcement duties.
LEO Threat	An individual who has a record of hostility and/or violence toward LEOs.
Misdemeanor	An offense punishable by incarceration, usually in a local confinement facility, for a period of which the upper limit is prescribed by statute in a given jurisdiction, typically limited to a year or less.
MUPU	Missing and Unidentified Persons Unit. A component of WSP.
N/A	Not applicable.
NCIC	National Crime Information Center.
NCIC 2000	An FBI initiative to upgrade the NCIC to better meet the needs of federal and state criminal justice agencies.

Term/Acronym	Definition
NICB	National Insurance Crime Bureau. WACIC provides information on impounded vehicles to NICB via NLETS.
NICS	National Insta-Check System.
NLETS	National Law Enforcement Telecommunication System. This is the system by which criminal justice information is shared between states.
OAC	Office of the Administrator for the Courts.
OBTS	Offender-Based Tracking System. This system, maintained by DOC, contains information on state prisoners.
Offender	An adult who has been convicted of a criminal offense.
On-Line Transactions	In this document, on-line refers to real-time transactions that are performed through direct connection to the system.
Person	A human being, or group of human beings considered a legal unit, having the lawful capacity to defend rights, incur obligations, prosecute claims, or be prosecuted or adjudicated.
Person of Interest	A person for whom a warrant has not been issued but who is being sought by a criminal justice agency. Examples include witnesses, suspects, and overdue motorists.
Probation	The conditional freedom granted by a judicial officer to an alleged or adjudged adult or juvenile offender, as long as the person meets certain conditions of behavior.
Program Transactions	In this document, program transactions refers to transactions that take place automatically from an application of one system to an application of another.
Provide the Ability to	Develop a fully functioning module, integrated with the remainder of the system, that performs the functionality addressed in the requirement.
RCW	Revised Code of Washington.
SCOMIS	Superior Court Management Information System.

Term/Acronym	Definition
Supervised Person	A person subject to adjudication or who has been adjudicated to be an offender who is under authorized and required guidance, treatment, and/or behavior regulation.
Unrestricted Criminal History	A report that addresses all arrests to which a person has been subject (i.e., not restricted to convictions only).
Vehicle	A motorized conveyance capable of transporting its operator. This includes automobiles, motorcycles, trucks, boats, farm and construction equipment, and airplanes.
VIN	Vehicle Identification Number.
Vulnerable Adult	A person 60 years or older who has the functional, mental, or physical inability to care for himself or herself.
WACIC	Washington Crime Information Center.
Wanted Person	A person sought by law enforcement authorities because an arrest warrant has been issued or because he or she has escaped from custody.
WASIS	Washington State Identification System - The state criminal history records computer system. WASIS also refers to the Identification Section of WSP.
Warrant	A writ or court order authorizing an arrest, seizure, or search or the performance of some other designated act.
WSP	Washington State Patrol.

APPENDIX B
SAMPLE SURVEY INSTRUMENT

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK
NETWORK INTERVIEW GUIDE/QUESTIONNAIRE

Name:	County/City:
Position:	Date:

I. ORGANIZATION AND BACKGROUND

A. Describe your current job functions relative to providing network, information systems, or communication services.

B. What organization(s) is(are) are responsible for establishing strategies, policies, and direction related to computing and networking?

C. How many end users of technology does your organization support? Are there other technology-oriented support organizations within the county/city?

D. Where are the technology users located? Are they primarily located in a single building, or are they geographically dispersed? Indicate the number of cities, building, and floors.

E. What is your level of involvement/interaction with state agencies? Which agencies do you, or your users, interact with? What state information/applications do your users access?

F. What methods/networks are currently used to access these state systems (ACCESS, dial-up, dedicated facilities, fax, telephone, mail, other)?

II. CURRENT ENVIRONMENT

A. Applications

1. Describe at a high level your county-wide information systems environment.

2. What computing system do you currently operate (mainframe, minicomputer, server, workstation, etc.)?

3. What operating systems are currently used (MVS, VM, OS400, OS/2, Windows, Windows NT, Macintosh, Unix, DOS, etc.)?

4. How many of each workstation type/operating system are installed?

5. How are the host application platforms networked (LANs, leased lines, dial up, front end processors, others)?

6. What, if any, networking restrictions are imposed by the existing applications?

7. Do your end users utilize E-mail? Is there a county-wide E-mail system?

8. Do users utilize other "groupware" applications, such as scheduling and Lotus Notes?

9. What office automation applications are used? Are there standards? How are these standard defined and enforced?

B. Networking

1. How do your users access state and county information systems (PC, fixed-function terminals, etc.)

2. Do your users have LANs? (Indicate the number of users on LANs, number with stand-alone intelligent workstations, and number with fixed-function devices.)

3. Which LAN topologies are implemented (ethernet, token ring, ATM, etc.)? How many of each LAN type are installed? What is the average number of users per LAN segment?

4. Are the LANs interconnected?

5. Do you utilize wiring hub and/or LAN switches (how many of each)?

6. What LAN wiring have you used (UTP type 3, type 5, coax, wireless, etc.)? What type of wiring is in each location?

7. Which network protocol(s) do you currently utilize (IPX, TCP/IP, SNA, Banyon vines, DECnet, others)?

8. How are LANs interconnected (bridges, routers, switches, etc.)?

9. Do you interconnect LANs between buildings?

10. What facilities do you use to interconnect buildings (leased lines, frame relay, ISDN, ATM, wireless, other)? At what speeds do these facilities operate?

11. Are your users connected to the Internet? How many users access the Internet daily? What are the primary and secondary reasons for Internet access?

12. What method do your users employ to connect to the Internet (dial-up, dedicated connection, other)?

13. Please include any network schematic that you have.

III. NETWORK MANAGEMENT AND ADMINISTRATION

A. Support Services

1. Is there a centralized help desk to assist users? What is the current help desk staffing level? How many calls does the help desk typically receive per day?

2. Do you have a problem tracking and managing the system?

3. Is there a person or group within the organization responsible for capacity planning and performance monitoring?

4. How are additions, moves, and changes to the network administered and controlled? What organization is responsible for managing this function?

B. Security

1. Do you have a network security policy and/or architecture?

2. Do you utilize security techniques such as encryption, access control/firewalls, others? If so, in what cases are these techniques used?

3. What level of application/system security have you implemented? Are there specific security products that you have implemented?

4. Do you utilize any form of third-party authentication services (Kerberos, DCE security, etc.)?

5. Do you provide dial-in access to your systems/network? What security measures have been implemented (unique key generation, dial back, users id/password)?

IV. CURRENT PLANS

A. What plans are currently in place, in process, or in discussion related to networking and information systems? What are the implications of the plan changes?

B. Please describe network-related projects regarding changing technology, additional functionality or bandwidth, increased security, or addition of new users and/or sites to the network.

C. Please describe application-related projects regarding new applications, major modifications to existing systems, re-hosting to open systems platforms, or Internet/intranet/WWW functionality.

D. Please describe other infrastructure projects related to building construction/remodeling, major work group moves, or changes in computing platforms?

E. Are there major user-initiated projects that will impact computing and communications in the county?

APPENDIX C

AGENCY TYPE CODES

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

AGENCY TYPE CODES

Type Code	Code Description	Lead Agency	Utilization Factor
911	Communications Center	WSP	1.00
AC	Appellate Courts	OAC	0.50
CA	County Attorney	WSP	0.25
CC	Community Corrections	DOC	1.00
CHO	County Health Office	DOH	0.50
DC	District Court	OAC	1.00
DL	Driver Licensing Office	DOL	1.00
DOC	Department of Corrections	DOC	1.00
DOH	Department of Health	DOH	0.50
EH	Environmental Health	DOH	0.50
FED	Federal Agency	WSP	0.50
LHD	Local Health District	DOH	0.50
MC	Municipal Court	OAC	1.00
PD	Police Department	WSP	0.50
PHO	Public Health Office	DOH	0.50
PR	Prison	DOC	1.00
SA	State Agency	WSP	0.50
SC	Superior Court	OAC	1.00
SHO	Satellite Health Office	DOH	0.50
SO	Sheriff's Office	WSP	0.50
SP	State Patrol	WSP	1.00
TC	Tribal Courts	OAC	0.50
VL	Vehicle Licensing Office	DOL	1.00
YS	Youth Services	WSP	0.50

APPENDIX D
COUNTY AND CITY INFORMATION

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
ADAMS	1.00	13,603		
			Othello	1
			Tokio	1.5
			Ritzville	1.5
ASOTIN	1.00	17,605		
			Clarkston	1.5
			Asotin	1.5
BENTON	0.75	112,560		
			Prosser	1
			Hanford	1
			Benton	1
			Kennewick	1
			Richland	1
			West Richland	1
CHELAN	0.75	52,250		
			Leavenworth	1.5
			Wenatchee	1
			Chelan	1.5
			Cashmere	1.5
CLALLAM	0.50	56,464		
			Neah Bay	1.5
			Sequim	1
			Clallam Bay	1
			Port Angeles	1
			Forks	1.5
CLARK	0.50	238,053		
			Vancouver	1
			Battleground	1
			Camas	1
			Ridgefield	1.5
			Washougal	1
			Yacolt	1.5
			Hazel Dell	1
			La Center	1.5
COLUMBIA	0.75	4,024		
			Dayton	1.5
COWLITZ	0.25	82,119		
			Woodland	1
			Kalama	1.5
			Kelso	1
			Longview	1
			Castle Rock	1
DOUGLAS	0.75	26,205		
			East Wenatchee	1
			Waterville	1.5
			Bridgeport	1.5
			Rock Island	1.5

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
FERRY	1.00	6,295		
			Republic	1.5
FRANKLIN	0.75	37,473		
			Pasco	1
			Connell	1.5
			Kahlotus	1.5
GARFIELD	0.75	2,248		
			Pomeroy	1.5
			Colton	1.5
			Uniontown	1.5
GRANT	0.75	54,758		
			Royal City	1.5
			Quincy	1.5
			Soap Lake	1.5
			Warden	1.5
			Grand Coulee	1.5
			Electric City	1.5
			Coulee City	1.5
			Ephrata	1
			Moses Lake	1
GRAYS HARBOR	0.50	64,175		
			Ocean Shores	1.5
			McCleary	1.5
			Oakville	1.5
			Westport	1.5
			Taholah	1.5
			Hoquiam	1
			Elma	1.5
			Aberdeen	1
			Cosmopolis	1.5
			Montesano	1
ISLAND	0.50	60,195		
			Langley	1
			Camano Island	1
			Freeland	1
			Oak Harbor	1
			Coupeville	1
JEFFERSON	0.50	20,146		
			Hadlock	1
			Port Townsend	1
KING	0.00	1,507,319		
			Brier	1
			Normandy Park	1
			Pacific	1
			Redmond	1
			Renton	1
			Mercer Island	1
			Snoqualmie	1
			Burien	1

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
KING	0.00	1,507,319		
			Fall City	1
			Medina	1
			Vashon Island	1
			SeaTac	1
			Beaux Arts	1
			North Bend	1
			Carnation	1
			Lake Forest Park	1
			Tukwila	1
			Seattle	1
			Algona	1
			Auburn	1
			Bellevue	1
			Bothell	1
			Des Moines	1
			Duvall	1
			Enumclaw	1
			Federal Way	1
			Issaquah	1
			Kent	1
			Kirkland	1
			Black Diamond	1
KITSAP	0.00	189,731		
			Rolling Bay	1
			Silverdale	1
			Bainbridge Island	1
			Bremerton	1
			Port Orchard	1
			Poulsbo	1
KITTITAS	0.50	26,725		
			Cle Elum	1.5
			Kittitas	1.5
			Roslyn	1.5
			Ellensburg	1
KLICKITAT	0.50	16,616		
			Goldendale	1.5
			White Salmon	1.5
LEWIS	0.00	59,358		
			Centralia	1
			Winlock	1.5
			Vader	1.5
			Toledo	1.5
			Pe Ell	1.5
			Napavine	1.5
			Morton	1.5
			Chehalis	1
			Mossyrock	1.5

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
LINCOLN	0.50	8,864		
			Sprague	1.5
			Davenport	1.5
			Temp	1.5
			Wilbur	1.5
			Almira	1.5
			Harrington	1.5
			Rearden	1.5
			Odessa	1.5
MASON	0.00	38,341		
			Shelton	1
			Belfair	1
OKANOGAN	0.75	33,350		
			Nespelem	1.5
			Conconully	1.5
			Winthrop	1.5
			Twisp	1.5
			Tonasket	1.5
			Elmer City	1.5
			Omak	1.5
			Coulee Dam	1.5
			Brewster	1.5
			Okanogan	1.5
			Oroville	1.5
PACIFIC	0.50	18,882		
			South Bend	1.5
			Ilwaco	1.5
			Long Beach	1.5
			Raymond	1.5
PEND OREILLE	1.00	8,915		
			Newport	1.5
			Ione	1.5
			Metaline Falls	1.5
PIERCE	0.00	586,203		
			Wilkeson	1
			Sumner	1
			Fort Lewis	1
			McNeil Island	1
			Eatonville	1
			Milton	1
			Roy	1
			Parkland	1
			Ruston	1
			McChord AFB	1
			Orting	1
			Bonney Lake	1
			Puyallup	1
			Steilacoom	1
			Ashford	1

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
PIERCE	0.00	586,203		
			Buckley	1
			Dupont	1
			Fife	1
			Fircrest	1
			Gig Harbor	1
			Tacoma	1
SAN JUAN	0.75	10,035		
			Friday Harbor	1.5
			Lopez Island	1.5
			Orcas Island	1.5
SKAGIT	0.00	79,555		
			Burlington	1
			Mount Vernon	1
			Sedro Woolley	1
			Concrete	1
			Anacortes	1
			La Conner	1
SKAMANIA	0.50	8,289		
			Stevenson	1.5
			North Bonneville	1.5
SNOHOMISH	0.00	465,462		
			Snohomish	1
			Woodinville	1
			Sultan	1
			Stanwood	1
			Mukilteo	1
			Lake Stevens	1
			Granite Falls	1
			Gold Bar	1
			Edmonds	1
			Everett	1
			Darrington	1
			Mountlake Terrace	1
			Monroe	1
			Mill Creek	1
			Marysville	1
			Bow	1
			Lynnwood	1
			Arlington	1
SPOKANE	1.00	361,364		
			Deer Park	1
			Medical Lake	1
			Liberty Lake	1
			Fairchild AFB	1
			Cheney	1
			Spokane	1
			Airway Heights	1

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
STEVENS	1.00	30,948		
			Northport	1.5
			Colville	1.5
			Springdale	1.5
			Chewelah	1.5
			Kettle Falls	1.5
THURSTON	0.00	161,238		
			Olympia	1
			Lacey	1
			Tumwater	1
			Littlerock	1
			Rainier	1
			Tenino	1
			Yelm	1
			Rochester	1
Unknown				
			Woodway	1.5
			Mattawa	1.5
			Silver Lake	1.5
WAHKIAKUM	0.50	3,327		
			Cathlamet	1.5
WALLA WALLA	1.00	48,439		
			Walla Walla	1
			Waitsburg	1.5
			Prescott	1.5
			College Place	1
WHATCOM	0.50	127,780		
			Blaine	1
			Everson	1
			Ferndale	1
			Lynden	1
			Sumas	1
			Bellingham	1
WHITMAN	1.00	38,775		
			Garfield	1.5
			Palouse	1.5
			Rosalia	1.5
			Tekoa	1.5
			Albion	1.5
			Pullman	1.5
			Colfax	1.5
			Oakesdale	1.5
YAKIMA	0.75	188,823		
			Granger	1
			Tieton	1
			Moxee City	1
			Mabton	1
			Zillah	1
			Wapato	1

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

COUNTY AND CITY INFORMATION

County Name	DTS Flag	Population	City Name	Cloud Flag
YAKIMA	0.75	188,823		
			Union Gap	1
			Toppenish	1
			Selah	1
			Grandview	1
			Sunnyside	1
			Yakima	1

APPENDIX E
PROJECT RISK ASSESSMENT MODEL

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

PROJECT RISK ASSESSMENT MODEL

A. PURPOSE

To provide a means for agencies, DIS, OFM and any other oversight entities to evaluate and monitor the risk components of information technology projects.

B. DESCRIPTION

The risk assessment contained in this appendix is designed to identify high-risk factors that may accompany large and small information technology projects. It is designed for use by project management and oversight personnel who have knowledge of the project and by agency personnel who have experience in evaluating projects of similar size and scope.

When high-risk factors are identified, they should raise a red flag to the agency and to oversight agencies. The flag indicates that a condition exists that could negatively impact project success. When the high-risk factor has been identified, the agency should prepare a plan addressing how it will manage the risk factor. Oversight agencies can then periodically review the project in light of these high risks to ensure that they are being managed properly and are not detrimental to the project.

The risk assessment is summarized in the Risk Assessment Worksheet (see EXHIBIT E-1, which follows this page). Instructions for using the worksheet are provided below.

C. INSTRUCTIONS

Information systems projects consist of many factors that increase or decrease the risk of the project. The Risk Assessment Worksheet provides a structured method for analyzing the risks of information systems projects. It should be completed by oversight personnel when evaluating the project.

Risks have been organized into eight categories: project management, customer involvement, organization, technology, scope, oversight, business impact, and cost-benefit. Each risk category contains five risk factors relating to the topic. These are described in subsection D, below.

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

PROJECT RISK ASSESSMENT

	Category	Risk Rating	x	Wgt.	Risk Score	Risk %
1.0	Project Management					
1.1	Project Management Experience	1 **2** 3 4	x	5	10	
1.2	Project Commitment	1 2 **3** 4	x	5	15	
1.3	Project Manager Authority	1 **2** 3 4	x	5	10	
1.4	Project Management Approach	1 **2** 3 4	x	5	10	
1.5	Project Management Relationships	1 2 **3** 4	x	5	15	
	Project Management					60%
2.0	Customer Involvement					
2.1	Customer Acceptance	1 2 **3** 4	x	5	15	
2.2	Customer Responsibility	1 2 **3** 4	x	5	15	
2.3	Customers on Project Team	1 **2** 3 4	x	5	10	
2.4	Customer Experience	1 **2** 3 4	x	5	10	
2.5	Customer Justification	1 **2** 3 4	x	5	10	
	Customer Involvement					60%
3.0	Organization					
3.1	Agency Experience	1 2 **3** 4	x	5	15	
3.2	Executive Management Involvement	1 **2** 3 4	x	5	10	
3.3	Management Cohesiveness	1 **2** 3 4	x	5	10	
3.4	Organizational Stability	**1** 2 3 4	x	5	5	
3.5	External Funding	1 **2** 3 4	x	5	10	
	Organization					50%
4.0	Technology					
4.1	Hardware Experience	1 **2** 3 4	x	5	10	
4.2	Software Experience	1 **2** 3 4	x	5	10	
4.3	Methodology Experience	1 **2** 3 4	x	5	10	
4.4	Quality Assurance	**1** 2 3 4	x	5	5	
4.5	Project Staff Technical Training	1 **2** 3 4	x	5	10	
	Technology					45%
5.0	Scope					
5.1	Project Scope Size	**1** 2 3 4	x	5	5	
5.2	Change Control Management	1 **2** 3 4	x	5	10	
5.3	Requirements Diversity	**1** 2 3 4	x	5	5	
5.4	Work Plan	**1** 2 3 4	x	5	5	
5.5	Available Resources	1 **2** 3 4	x	5	10	
	Scope					35%
6.0	Oversight					
6.1	Monitoring Process	1 **2** 3 4	x	5	10	
6.2	DIS Involvement	**1** 2 3 4	x	5	5	
6.3	Procurement Process	1 **2** 3 4	x	5	10	
6.4	Milestone Reviews	1 **2** 3 4	x	5	10	
6.5	Status Reporting	1 **2** 3 4	x	5	10	
	Oversight					45%

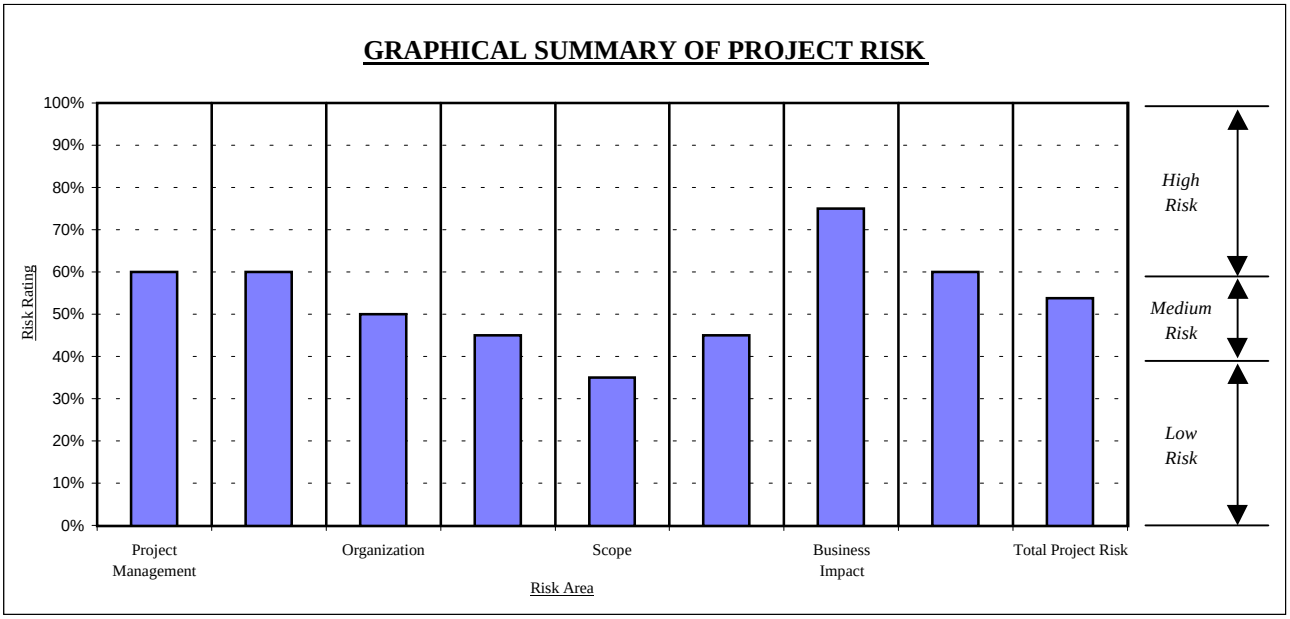
ECG MANAGEMENT CONSULTANTS

STATE OF WASHINGTON
JUSTICE INFORMATION NETWORK

PROJECT RISK ASSESSMENT

	Category	Risk Rating	x	Wgt.	Risk Score	Risk %
7.0	Business Impact					
7.1	Agency Mission/Program Impact	1 2 3 **4**	x	5	20	
7.2	Customer Impact	1 2 **3** 4	x	5	15	
7.3	Change in Customer Service	1 **2** 3 4	x	5	10	
7.4	Technology Dependence	1 2 **3** 4	x	5	15	
7.5	Performance Requirements	1 2 **3** 4	x	5	15	
	Business Impact					75%
8.0	Cost-Benefit					
8.1	Budget Size	1 **2** 3 4	x	5	10	
8.2	Achievable Benefits	1 **2** 3 4	x	5	10	
8.3	Economic Justification	1 2 **3** 4	x	5	15	
8.4	Elapsed Time	1 2 **3** 4	x	5	15	
8.5	Cost Control	1 **2** 3 4	x	5	10	
	Cost-Benefit					60%
	TOTAL PROJECT RISK				430	54%

GRAPHICAL SUMMARY OF PROJECT RISK



ECG MANAGEMENT CONSULTANTS

Rate each risk factor on a scale of 1 to 4, where 1 represents little risk and 4 represents high risk. Answering a question "yes" implies lower risk; answering it "no" implies higher risk.

1	2	3	4
<----------			---------->
YES			NO
Limited Risk	Some Risk	Significant Risk	High Risk

After each risk factor in a category has been rated, add the scores in the category and place the score in the "Risk Score" column next to the category on the Risk Assessment Worksheet. Multiply the total score by 5 to get a percentage rating for the category and place the percentage in "Risk %" column next to the category on the Risk Assessment Worksheet. The number of high-risk factors (ratings of "4") should also be recorded in the Risk Rating space provided next to each category. Finally, the bar chart should be completed by graphing each percentage in the "bar" next to each category.

D. RISK ASSESSMENT CATEGORIES AND EVALUATION FACTORS

1. Project Management

1.1 Project Management Experience - Is the project manager experienced in successfully managing projects of similar size and complexity?

1.2 Project Commitment - Has the project manager been assigned to the project full-time for its duration?

1.3 Project Manager Authority - Does the project manager have authority over the necessary resources to conduct the project, and is the project manager held accountable and responsible for the project's success?

1.4 Project Management Approach - Does the project manager propose to use proven project management techniques?

1.5 Project Management Relationships - Does the project manager have good working relationships with information systems staff, customer team management, customer personnel, etc.?

2. Customer Involvement

2.1 Customer Acceptance - Are customers involved in analysis, design, and review of the project in a structured way?

2.2 Customer Responsibility - Are customers responsible and accountable for the project's success?

2.3 Customers on Project Team - Does the project team include customers who are dedicated to the project?

2.4 Customer Experience - Are the customers assigned to or working with the project team knowledgeable regarding the business area involved?

2.5 Customer Justification - Did the system customers prepare or assist in preparing the feasibility study and other justification materials?

3. Organization

3.1 Agency Experience - Does the agency have experience in developing projects of similar size and scope?

3.2 Executive Management Involvement - Does the agency's executive management support the project?

3.3 Management Cohesiveness - Does the agency's management, responsible for the project, work together effectively as a team?

3.4 Organizational Stability - Is the organization stable? Is there little management turnover or structural change? Is attrition low?

3.5 External Funding - If funding from external sources (e.g., federal funding) will pay for the project, are these funding sources reasonably assured?

4. Technology

4.1 Hardware Experience - Does the agency have experience using the proposed hardware in projects of similar size and scope?

4.2 Software Experience - Does the agency have experience using the proposed software in projects of similar size and scope?

4.3 Methodology Experience - Does the agency have experience using the proposed development methodology in projects of similar size and scope?

4.4 Quality Assurance - Is a comprehensive quality assurance program in place using statistical methods to measure the quality of processes and results?

4.5 Project Staff Technical Training - Have project staff received adequate training in the hardware, software, methodology, or business function involved or included in the project?

5. Scope

5.1 Project Scope Size - Is the project scope well defined and of manageable size?

5.2 Change Control Management - Are comprehensive change control procedures in place and strictly followed?

5.3 Requirements Diversity - Are system requirements simple and limited to a single functional group?

5.4 Work Plan - Has a work plan been prepared in detail using a phased approach, and is it strictly followed in managing project tasks?

5.5 Available Resources - Are resources (personnel, computer, etc.) available as needed?

6. Oversight

6.1 Monitoring Process - Has a monitoring process been established that addresses high-risk factors and significant variances in schedule and budget?

6.2 DIS Involvement - Has DIS been actively involved in the planning and review of this project?

6.3 Procurement Process - Is the procurement approach comprehensive, and does it use a structured Request for Proposal/Request for Information and evaluation process? Are vendors asked to benchmark and prove their claims?

6.4 Milestone Reviews - Are reviews conducted by end customers and management regularly throughout the project's life cycle?

6.5 Status Reporting - Are status reports planned to be presented to customers and management on a regular basis? Is feedback from these reports considered and incorporated into project planning?

7. Business Impact

7.1 Agency Mission/Program Impact - Is the impact on the agency's mission and programs predictable?

7.2 Customer Impact - Will the end customer's daily routine (manual or automated) remain the same with the new system as is presently the case?

7.3 Change in Customer Service - Will the way the agency interacts with its external customers remain the same under the new system as it is now?

7.4 Technology Dependence - Does the project have reasonable safeguards to ensure the success of new technology?

7.5 Performance Requirements - Are the system performance requirements reasonably achievable?

8. Cost-Benefit

8.1 Budget Size - Does the proposed budget appear reasonable compared to that of other projects of similar size and complexity?

8.2 Achievable Benefits - Are the benefits used to justify the project realistic and achievable? Do they provide significant cost savings, increased productivity, increased revenue, or additional service?

8.3 Economic Justification - Is the economic justification well defined and does it justify the project?

8.4 Elapsed Time - Does the project schedule reflect a reasonable, achievable time frame or does the time frame span several years?

8.5 Cost Control - Are cost control measures in place to ensure optimal use of the project budget?